ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ
ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ (ΠΡΩΗΝ Ε.Π.Δ.Ο.)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ:

«Ασφάλεια Πληροφοριακών Συστημάτων & Ανάλυση Ευπαθειών Ιστοσελίδων Τ.Ε.Ι. Μεσολογγίου»

Εισηγητής: Δρ. Γαρμπής Αριστογιάννης

Σπουδαστές:
Παπαδομανωλάκης Κυριάκος ΑΜ: 14916
Μητρόπουλος Περικλής ΑΜ: 14875

Μεσολόγγι 2017

Περιεχόμενα

1) Θεωρητική Ανάλυση

1.1) Εισαγωγή

Η επιστήμη της πληροφορικής θεωρείται το γνωστικό αντικείμενο που ασχολείται με διάφορα πεδία των πληροφοριακών συστημάτων όπως *επεξεργασία, ανάλυση, ασφάλεια, ανάκτηση, συλλογή, εγγραφή, αποθήκευση κ.α.* Εφόσον τα πληροφοριακά συστήματα προορίζουν τις παραπάνω διαδικασίες, βρίσκουμε σκόπιμο να αναλύσουμε στα πλαίσια μιας πτυχιακής εργασίας την ασφάλεια και προστασία πληροφοριακών συστημάτων (υπολογιστών, δικτύων) θέλοντας να αποφύγουμε πιθανούς ψηφιακούς εγκληματολογικούς κινδύνους και απειλές εξελιγμένων κρυπτογραφιών.

Τα πληροφοριακά συστήματα παρέχουν μια σύνδεση επικοινωνιακής συνεργασίας ανάμεσα στον άνθρωπο και τον υπολογιστή μέσω δεδομένων και διαφόρων τεχνολογικών διαδικασιών. Απώτερος σκοπός είναι η τέλεια υποστήριξη για απλούς χρήστες έως και ανθρώπινο δυναμικό μεγάλων επιχειρήσεων στη διαχείριση λήψης σημαντικών τους αποφάσεων.

Μια ακόμα συσχέτιση με τα ΠΣ είναι η διαχείριση βάσης δεδομένων και δραστηριοτήτων μέσω διαφόρων λογισμικών (softwares) τα οποία δημιουργούν και συντηρούν ΒΔ και δραστηριότητες. Το σύστημα διαχείρισης βάσης δεδομένων είναι επίσης και ένας διαχειριστής αρχείων (file manager) ο οποίος διαχειρίζεται δεδομένα σε ΒΔ παρά αρχεία σε συστήματα αρχείων (τα οποία αντιστοιχούν σε άλλες μορφές ΒΔ).

Η πολιτική της ασφάλειας ΠΣ είναι απλή και έχει στόχο να προστατεύει τα συστήματα από κάθε είδους κίνδυνο. Η διαδικασία για τη σχεδίαση πολιτικής ασφαλείας δεν πρέπει να εμποδίζει τη λειτουργία των ΠΣ, αντίθετα πρέπει να εφαρμόζει κάποιους κανόνες και αρχές για άμυνα σε βάθος. Η βασική στιγμή για τη διαδικασία της σχεδίασης ασφαλών πολιτικών είναι η εντόπιση εμπιστευτικών πληροφοριών οι οποίες πρόκειται να χρησιμοποιηθούν και να προστατευθούν. Άλλοι όροι που πρέπει να υπάρχουν για μια αξιόπιστη πολιτική της ασφάλειας είναι οι έννοιες της *αυθεντικότητας, εγκυρότητας, μοναδικότητας* και της *μη αποποίησης,* για της οποίες θα αναφερθούμε εκτενώς.

1.2) Σκοπός της Πτυχιακής Εργασίας

Σκοπός της συγκεκριμένης πτυχιακής είναι η ευαισθητοποίηση των χρηστών καθώς και των διαχειριστών των πληροφοριακών συστημάτων (network-server Administrator) σε θέματα ψηφιακής ασφάλειας. Με αυτό τον τρόπο θα μπορούν να ενημερωθούν όλοι και να αποκτήσουν γνώση για το πως λειτουργούν τα πληροφορικά συστήματα στη σημερινή κοινωνία με την εξέλιξη της ψηφιακής τεχνολογίας.
Στο τομέα της ψηφιακής ασφάλειας να ενημερώσουμε την εξέλιξή της και να παροτρύνουμαι τους άμεσα εμπλεκόμενους στην συνεχή παρακολούθηση των διαχειριζόμενων συστημάτων καθώς και την συνεχή αναβάθμιση αυτών ώστε να μην είναι ευάλωτα στιςσύχρονες επιθέσεις. Η ανάλυση που πραγματοποιήθηκε χωρίζεται σε δύο στάδια.
Το $1^{ο}$ στάδιο είναι η συλλογή πληροφοριών (Information Gathering) και $2^{ο}$ η ανεύρεση επαθειών (Vulnerability Assesment) στις λειτουργικές ηλεκτρονικές διευθήνσεις ολόκληρου του Ιδρύματος.
Στην πρώτη ενότητα θα σας παρουσιάσουμε κάποιες βασικές λεπτομερειες ενός πληροφοριακού συστήματος και μία γενική αναφορά σε διάφορες απειλές.
Στη δεύτερη ενότητα αναφέρουμε τις ευπάθειες που βρήκαμε μετά απο την ανεύρεση των ευπαθειών με δύο προγράμματα και τις λεπτομέρειες που αναφέρονται στις αναφορές αυτές.
Προς το τέλος της πτυχιακής έχουμε τις φωτογραφίες από τα προγράμματα και τις αναφορές τους.

1.3) Ιστορική αναδρομή & αναφορά σε ιούς

Η ιστορία της επιστήμης της ασφάλειας πληροφοριακών συστημάτων ξεκινάει λίγο πριν εξαπλωθεί η σύγχρονη επιστήμη των υπολογιστών κάπου στον εικοστό αιώνα. Η πρώτη δημοσίευση είναι γνωστό πως προήλθε από μία ομάδα εργασίας του συμβουλίου αμυντικής επιστήμης του υπουργείου άμυνας των Η.Π.Α. Ήθελαν να εξετάσουν τότε ποια θα είναι τα προβλήματα όταν θα χρειαστεί να συνδεθούν δύο υπολογιστές εξ αποστάσεως με τη χρήση τερματικών. Για να προσεγγίσουν τότε λύσεις προβλημάτων ασφαλείας έπρεπε να απομονώσουν (κλειδώσουν σε ιδιωτικό χώρο) τον κεντρικό υπολογιστή ώστε να ελέγχουν την πρόσβαση σε αυτόν. Αυτό δεν ήταν πρακτικά εφικτό να συνεχιστεί κι έτσι αργότερα αναγκάστηκαν να βρουν νέους τρόπους και μεθόδους για ασφάλεια.

Οι ιοί εμφανίστηκαν όταν ξεκίνησε να εξαπλώνει τα πρώτα της βήματα η σύγχρονη επιστήμη των υπολογιστών, γύρω στη δεκαετία του ’70, με τον πρώτο εν ονόματι “Creeper” καθώς και το πρώτο διαδικτυακό σκουλήκι (worm) με όνομα “Morris” λίγο πριν το 2000, το οποίο πρόσβαλλε χιλιάδες συστήματα και υπολογιστές.

Ο πρώτος ιός που αναφέρεται ως πιο εξαπλωμένος εκτός του συστήματος, υπήρξε ο Elk Cloner, ο οποίος δημιουργήθηκε από τον δεκαπέντε ετών Richard Skrenta, για υπολογιστές Apple II[1] με λειτουργικό σύστημα Apple DOS 3.3. Ο δεκαπεντάχρονος Richard αποθήκευσε τον ιό του σε μία δισκέτα και την έδωσε σε φίλους και γνωστούς του. Πρέπει να σημειωθεί ότι οι υπολογιστές εκείνης της εποχής δε διέθεταν σκληρό δίσκο στο σύστημά τους, έτσι οι ανταλλαγές δισκετών μεταξύ χρηστών ήταν αρκετά συχνό φαινόμενο. Όταν ο υπολογιστής εκκινούσε στο σύστημά του τη μολυσμένη αυτή δισκέτα, ο ιός αντιγραφόταν από μόνος του σε οποιαδήποτε άλλη δισκέτα ήταν συνδεδεμένη στον υπολογιστή. Μετά από κάποιον αριθμό εκκινήσεων από μολυσμένη δισκέτα, ο υπολογιστής εμφάνιζε ένα μήνυμα υπό μορφή στίχων. Ο συγκεκριμένος ιός δεν είχε καταστροφικές προθέσεις και ο δημιουργός του Skrenta τον έφτιαξε ως αστείο. Παρόλα αυτά, ο έφηβος κατάφερε να τον διαδώσει στους υπολογιστές αρκετών συμμαθητών του καθώς και στον καθηγητή των μαθηματικών, με αυτό εξασφάλισε μία θέση στην ιστορία των ιών.

Ο πρώτος ιός που εμφανίστηκε στους προσωπικούς υπολογιστές ήταν ο ιός Brain, ο οποίος ήταν γνωστός και με άλλα ονόματα όπως: Ashar, ©Brain, Clone, Nipper κ.α. Δημιουργήθηκε στο Πακιστάν το 1986 από δύο αδερφούς Basit και Amjad Farooq Alvi. Ο συγκεκριμένος ιός προσέβαλε τον τομέα εκκίνησης (boot sector) του σκληρού δίσκου.

Από τότε έως σήμερα έχουν δημιουργηθεί και κυκλοφορήσει χιλιάδες είδη ιών, εκ των οποίων οι περισσότεροι προκαλούν φθορές στο υπολογιστικό σύστημα ή δίκτυο στο οποίο εισχωρούν. Στα πρώτα χρόνια του εικοστού πρώτου αιώνα εκτιμάται ότι με τη ραγδαία αύξηση του διαδικτύου δημιουργήθηκαν και ανακαλύφθηκαν πάνω από 700.000 ιοί. Ωστόσο αυτοί ταξινομούνται σε δύο μεγάλες κατηγορίες, ανάλογα με το σημείο του υλικού/λογισμικού που μολύνουν και ανάλογα με τον τρόπο που πραγματοποιούν τη

[1] Ο Apple II ήταν ένας 8-bit οικιακός υπολογιστής, ο οποίος κυκλοφόρησε από την Apple τον Απρίλιο του 1977 καθώς και ο Apple II + που κυκλοφόρησε λίγους μήνες αργότερα. Αποτέλεσαν τους πρώτους ηλεκτρονικούς υπολογιστές μαζικής παραγωγής για την συγκεκριμένη εταιρεία.

μόλυνσή τους. Παρακάτω θα αναλύσουμε σχετικά πράγματα για αυτούς, καθώς και τρόπους δράσης, αντιμετώπισης αλλά και πως διαδίδονται.

1.4) Βασικές αρχές των ΠΣ

Υπάρχουν κάποιες βασικές αρχές στη χρήση και λειτουργία των ΠΣ που οφείλουν να ικανοποιούν κάποιες απαιτήσεις τις οποίες θα αναφέρουμε παρακάτω:

- Οι μηχανισμοί ασφαλείας πρέπει να μην επιβαρύνουν τη συνολική αποτελεσματικότητα του συστήματος, όμως εάν αυτό δεν ισχύει τότε πρέπει να υπάρξουν αλλαγές ώστε η απόδοση και η ασφάλεια να βρίσκονται σε ισορροπία.
- Η διακίνηση εμπιστευτικών πληροφοριών προς τρίτους θα γίνεται επιτρεπτή μετά την ολοκλήρωση της εγγραφής άδειας του ενδιαφερόμενου.
- Η διαχείριση πληροφοριών θα πρέπει να πραγματοποιείται από εξουσιοδοτημένο προσωπικό.
- Τα δικαιώματα πρόσβασης πρέπει να προσδιορίζονται με ξεχωριστές και ανεξάρτητες διαδικασίες από αυτές του σταδίου υλοποίησης του συστήματος. Ο καθορισμός των διαδικασιών αυτών πραγματοποιείται σε νομοθετικό, οργανωτικό και δομικό επίπεδο.

Τα παραπάνω σημαίνουν ότι μια αποδοτική λειτουργία σε συνδυασμό με τη σωστή ανάπτυξη των ΠΣ είναι μια διαδικασία που εμπεριέχει μια δόμηση πλαισίου ασφαλείας, το οποίο παρέχει εξασφάλιση σε απαιτήσεις όπως *διαθεσιμότητα, μυστικότητα* και *ορθότητα* στα περιεχόμενα των πληροφοριών.

1.5) Σχεδιασμός Ασφαλών Πληροφοριακών Συστημάτων

Οι απαιτήσεις ασφαλείας ενός συστήματος καθορίζονται από κάποιες διαδικασίες, όταν αρχικώς καταγράφονται οι θεωρίες για τον καλύτερο δυνατό σχεδιασμό του. Μέσα στις διαδικασίες αυτές, οι μηχανισμοί ασφαλείας που μας απασχολούν, αναπτύσσονται στα τελευταία επίπεδα, μετά την υλοποίησή τους, με σκοπό να αντιμετωπιστούν τα πιθανά προβλήματα που προκύπτουν από τα προηγούμενα στάδια λειτουργίας. Το παραπάνω θεώρημα περιβάλλεται από διάφορα σοβαρά μειονεκτήματα και απειλές όπως:

- Συνέπειες των παραβιάσεων του συστήματος που προηγήθηκαν κατά τη διάρκεια ενσωμάτωσης των διαδικασιών ασφαλείας και πως αυτές θα αντιμετωπιστούν πλήρως.
- Αδυναμία της αναθεώρησης του συνολικού σχεδιασμού.
- Δυσκολία της ενσωμάτωσης των διαδικασιών ασφαλείας στο φυσικό σχεδιασμό.
- Φόρτος στον προγραμματιστικό τομέα υλοποίησης των τμημάτων του λογισμικού.
- Δυσχρηστία ατόμων τα οποία δεν έχουν την εξοικείωση και την εμπειρία ώστε να τηρήσουν τις διαδικασίες και τους κανόνες ασφαλείας του συστήματος.

- Επιπρόσθετο κόστος για αγορά υπολογιστικού εξοπλισμού και αντίστοιχου λογισμικού.

Τα παραπάνω προβλήματα μπορούν να εξαλειφθούν ή να μην εμφανιστούν καν, εάν υπάρξει έγκαιρη θεώρηση στις απαιτήσεις ασφάλειας του συστήματος. Η μελέτη τους και η υλοποίησή τους πρέπει να εφαρμόζονται ταυτόχρονα με όλα τα επίπεδα κύκλου ζωής ενός ΠΣ. Με την παραπάνω στρατηγική γίνεται εφικτό να υπάρχουν μετασχηματισμοί και αλλαγές σε ροές δεδομένων, εξοπλισμών και περιβάλλοντος λειτουργίας του συστήματος χωρίς να χρειάζεται ανασυγκρότηση το όλο οικοδόμημά του.

Ο ρόλος του πληροφοριακού συστήματος μέσα σε μια επιχείρηση απαιτεί ασφάλεια και προστασία, γι' αυτό οφείλεται να δίνεται βαρύτητα σε κάποια βασικά στοιχεία όταν σχεδιάζεται ένα ΠΣ. Τα σημαντικότερα στοιχεία είναι τα ακόλουθα:

- Προσοχή και εστίαση σε επιμέρους στοιχεία του συστήματος, όχι αντιμετώπιση σαν μία ολότητα.
- Η προστασία αφορά κάθε είδους κίνδυνο, είτε αυτός είναι τυχαίος είτε γίνεται με σκοπιμότητα.
- Η ασφάλεια του συστήματος, από τη μία συνδέεται με τεχνικές διαδικασίες και διοικητικά μέτρα, ενώ από την άλλη υπάρχουν οι ηθικές αντιλήψεις και αρχές.
- Η προστασία δεν πρέπει να παρεμβάλλεται ως εμπόδιο στη λειτουργικότητα του συστήματος, αντιθέτως πρέπει να μην επιβαρύνει τη χρήση του αλλά ταυτόχρονα να παρέχει υπηρεσίες υπεράσπισης οποιαδήποτε στιγμή κριθεί αναγκαίο.

Επίσης, υπάρχουν τρεις αρχές που λειτουργούν ως καθοδηγήτριες για το σχεδιασμό ασφαλών ΠΣ, οι οποίες είναι:

1. **Άμυνα εις βάθος** (Defense in Depth). Αυτό σημαίνει ότι απαιτούνται διαδικασίες πολλαπλών ελέγχων προτού το πρόσωπο που δεν έχει άδεια δικαιωμάτων εξουσιοδότησης αποκτήσει πρόσβαση στο ΠΣ.
2. **Αντικατάσταση** (Duplication). Αυτή η αρχή στηρίζεται στην αναγκαία συνεχής ροή λειτουργίας ενός ΠΣ, έστω κι αν κάποιο υποσύστημα του σταματήσει να λειτουργεί. Επιπροσθέτως, η αντικατάσταση είναι σημαντικά χρήσιμη διότι βοηθάει στο να ανιχνευτούν πιθανά λάθη επεξεργασίας πληροφοριών.
3. **Αποκέντρωση** (Dispersion). Η συγκεκριμένη αρχή βασίζεται στην ιδέα πως η ολοκληρωτική καταστροφή ενός αποκεντρωμένου ΠΣ χρειάζεται πολλαπλές επεμβάσεις.

1.6) Ορισμός Πληροφοριακού Συστήματος & Προϋποθέσεις Ασφάλειας.

Κατ' αρχάς, πληροφοριακό σύστημα εννοείται ένας αριθμός στοιχείων τα οποία αλληλεπιδράν μεταξύ τους και συνεργάζονται για ένα τελικό αποτέλεσμα ώστε να επιτευχθεί μια συγκεκριμένη λειτουργία. Τα στοιχεία αυτά είναι τα εξής ακόλουθα:

1) Άνθρωπος, ο οποίος είναι ο δημιουργός των ΠΣ και τα υλοποιεί έτσι ώστε να λειτουργούν προς όφελός του και να τον εξυπηρετούν στο έπακρον.
2) Πληροφορία, την οποία ο άνθρωπος ζητάει να αποκτήσει ανελλιπώς.
3) Πληροφορική, επιστήμη η οποία στοχεύει στην επεξεργασία της πληροφορίας.

Απλούστερα, ΠΣ ονομάζεται ένα οικοδόμημα που αποτελείται από υλικά, λογισμικά, μέσα αποθήκευσης, δεδομένα και σε συνδυασμό με τους ανθρώπους – χρήστες, επιτυγχάνονται τα λειτουργικά βήματα που πρέπει.

Ο ρόλος του ΠΣ, για παράδειγμα σε μια επιχείρηση, απαιτεί αυστηρά μέτρα ασφαλείας και προστασίας, επομένως οι λειτουργίες του πρέπει να προστατεύονται από οποιαδήποτε μορφή απειλής και κινδύνου δίχως να βρίσκει εμπόδια η πληροφορία, δηλαδή η ροή της να κυλάει συνεχόμενα και ομαλά δίχως διακοπές.

Αναγκαία πράξη για μια τέλεια ασφάλεια, ακούει στην ύπαρξη ενός συνόλου απαιτήσεων – προϋποθέσεων που πρέπει πάντα να εκτελούνται, να μην απουσιάζουν και να μην αγνοούνται.

Οι προϋποθέσεις για την ασφάλεια των πληροφοριακών συστημάτων βασίζονται σε τρεις σημαντικές και αναγκαίες ιδέες (*ακεραιότητα (integrity), διαθεσιμότητα (availability) και εμπιστευτικότητα (confidentiality)*) ώστε να εφαρμοστεί μια ορθή και πλήρης λειτουργία ενός ΠΣ.

- **Ακεραιότητα** (Integrity), η οποία είναι υπεύθυνη στο να διατηρούνται τα δεδομένα ενός ΠΣ σε μια ακέραια και ασφαλή κατάσταση δίχως να μπορέσουν να επηρεαστούν από κάποιες ανεπιθύμητες τροποποιήσεις μη εξουσιοδοτημένων χρηστών, καθώς και την αποτροπή αυτών στη χρήση δικτύων και υπολογιστών του συστήματος δίχως την έγκριση με σχετική άδεια. Το χαρακτηριστικό (πρόβλημα) στην ακεραιότητα είναι πως δεν μπορεί να διευκρινιστεί απόλυτα για τον λόγο του ότι ο καθένας ενδέχεται να το ερμηνεύσει διαφορετικά και γι' αυτό κάποιες βασικές έννοιες της ακεραιότητας ακούν στα ονόματα *ακρίβεια, ορθότητα, συνέπεια, τροποποίηση μόνο με αποδεκτούς τρόπους από εξουσιοδοτημένα πρόσωπα και από εξουσιοδοτημένες διεργασίες*.

- **Διαθεσιμότητα** (Availability), η οποία είναι υπεύθυνη για να εξασφαλίζει στους χρήστες ότι τα δεδομένα, τα δίκτυα και οι υπολογιστές θα είναι διαθέσιμα οποιαδήποτε στιγμή θελήσουν εκείνοι. Όμως, μερικές φορές υπάρχει περίπτωση τα ΠΣ να απειληθούν και έτσι θα κληθούν να αντιμετωπίσουν τη λεγόμενη DOS attack (επίθεση άρνησης υπηρεσιών) που έχει ως στόχο να αφήσει εκτός λειτουργίας τον αρχικό σκοπό της διαθεσιμότητας όσο το δυνατόν περισσότερο χρόνο. Επίσης, η ενέργεια της DOS attack δεν έπεται ότι προέρχεται από εχθρικές επιθέσεις.

- **Εμπιστευτικότητα** (Confidentiality), η οποία είναι υπεύθυνη στο να μην αποκαλύπτει σημαντικές και ευάλωτες πληροφορίες σε χρήστες οι οποίοι δεν κατέχουν τα απαραίτητα εξουσιοδοτημένα ατομικά δικαιώματα που απαιτεί το σύστημα.

1.7) Απειλές & Μέθοδοι Ασφαλείας

Όπως ειπώθηκε πιο πάνω, η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών και δεδομένων κρούει τον κώδωνα του κινδύνου για το Πληροφοριακό Σύστημα διότι εκτίθεται η ασφάλεια. Όταν το νομικό αυτό δικαίωμα ριψοκινδυνεύει και γίνεται ευάλωτο τότε υπάρχει ευπαθή άμυνα που σημαίνει πως κάποιος τρίτος έχει την ικανότητα να εκμεταλλευτεί αυτό το μειονέκτημα και να προκαλέσει σχετικές φθορές και απώλειες στο σύστημα.

Θεωρείται πως όταν ένα σύστημα παραβιασθεί από κάποιο μη εξουσιοδοτημένο πρόσωπο εκμεταλλεύοντας την ευπάθεια, διαπράττει επίθεση. Αυτό πρέπει να εξαλειφθεί στο έπακρο με διαρκή και συνεχή συστηματικό έλεγχο. Αυτός ο έλεγχος είναι ένα από τα πιο προτεινόμενα προστατευτικά μέτρα που μπορεί να υλοποιηθεί μέσω ενεργειών, είτε συσκευών, είτε τεχνικών διαδικασιών.

Τα ΠΣ περιέχουν τρία αντικείμενα και τέσσερα είδη απειλών τους. Τα αντικείμενα ακούν στα ονόματα *υλικό, λογισμικό και δεδομένα* ενώ οι απειλές ακούν στα ονόματα *διακοπή, παρεμπόδιση, πλαστοποίηση και τροποποίηση*, στα οποία θα εξετάσουμε τις έννοιες τους παρακάτω.

- **Διακοπή (Interruption)**. Με τη διακοπή σημαίνει πως τα αντικείμενα που αναφέραμε παραπάνω δεν είναι στη διάθεση χρήσης και αυτό γιατί μάλλον χάνονται. Αυτό μπορεί να συμβεί όταν κάποιος προσπαθήσει να καταστρέψει τη συσκευή αυτή ή να διαγράψει πρόγραμμα με αρχεία και δεδομένα ώστε να αποσκοπήσει στη δυσλειτουργικότητα του συστήματος.
- **Παρεμπόδιση (Interception)**. Με την παρεμπόδιση σημαίνει ότι κάποια πρόσωπα που δεν έχουν δικαίωμα εξουσιοδοτημένης πρόσβασης έχουν αποκτήσει αυτό το προνόμιο για αυτό το σύστημα. Δεν είναι αναγκαίο αυτά τα πρόσωπα να είναι απαραίτητα άτομα, μπορεί να είναι είτε προγράμματά τους, είτε κάποιο άλλο πληροφοριακό σύστημα. Αυτή η αποτυχία μπορεί να προέλθει από την παράνομη αντιγραφή προγραμμάτων ή δεδομένων, όμως μπορεί να προέλθει και από υποκλοπές συνομιλιών ώστε να αποκτηθούν διάφοροι κωδικοί που είναι απαραίτητοι για την πρόσβαση στο εκάστοτε δίκτυο. Μια τέτοια απατεωνιά αποκαλύπτεται σχετικά γρήγορα και εύκολα από κάποιον έμπειρο χρήστη και γνώστη του συστήματος όμως αν ο υποκλοπέας είναι προσεκτικός και έμπειρος τότε μπορεί να εξαλείψει εντελώς τα ίχνη της ύπαρξής του.
- **Πλαστοποίηση (Fabricate)**. Με την πλαστοποίηση σημαίνει πως κάποια ομάδα μη εξουσιοδοτημένων χρηστών έχει την ικανότητα να πλαστογραφήσει αρχεία δεδομένων σε ένα ΠΣ. Οι εισβολείς μπορούν να κάνουν αλλαγές σε εγγραφές στις βάσεις δεδομένων όμως γρήγορα σε μικρό χρονικό διάστημα μπορεί να διαπιστωθεί πρακτικά από τους εξουσιοδοτημένους πως όντως αυτές οι εγγραφές είναι πλαστές, εκτός και αν οι παρανομείς είναι τόσο περίτεχνοι που τα χαρακτηριστικά δε διαφέρουν καθόλου από τα γνήσια αντικείμενα.
- **Τροποποίηση (Modification)**. Αυτό ταιριάζει πάνω-κάτω με την πλαστοποίηση και σημαίνει πως όταν μια μη εξουσιοδοτημένη ομάδα συνεχίσει μετά την εισβολή προσπελάζοντας δεδομένα και ανακατέψει αρχεία τότε έχει καταφέρει το σκοπό της. Εκτός του ότι μπορεί να αλλάξει τις εγγραφές σε μια βάση δεδομένων (όπως στην πλαστοποίηση), έχει τη δυνατότητα ακόμα να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί

καθήκοντα με το συμφέρον των εισβολών. Επίσης, υπάρχει δυνατότητα να διαπράξουν τροποποιήσεις οι οποίες να προσφέρουν αδυναμίες στο υλικό μέρος του συστήματος από την πλευρά των κατόχων ως όφελος των παρανόμων.

Υπάρχουν τρόποι ασφαλείας που ανά διαστήματα χρησιμοποιούνται και ως βάση αυτών, συνεχώς ανανεώνονται και δημιουργούν μηχανισμούς για τα μέτρα προστασίας που συνδυάζονται για να δώσουν μοντέλα ασφαλείας. Κάποια από τα πιο γνωστά μοντέλα είναι τα εξής:

- **Μοντέλα καταλόγου**. Υπάρχει μια σχετική λίστα με καταγεγραμμένα θέματα που αφορούν το τι πρέπει να γίνει ώστε να θεωρηθεί ένα ΠΣ ασφαλές από τους κινδύνους που το απειλούν.
- **Μοντέλα κιβωτισμού**. Υπάρχει μια σειρά από ομόκεντρους που προστατεύουν δεδομένα κατά τη διάρκεια της εμφάνισής τους καθώς και ότι αντίστοιχο υπάρχει από το ανθρώπινο δυναμικό που χειρίζεται το υπολογιστικό κέντρο κάποιας εκάστοτε επιχείρησης.
- **Μοντέλα του πίνακα**. Υπάρχει ένας πίνακας τριών διαστάσεων ο οποίος απεικονίζει σημαντικά θέματα που διαφέρουν μεταξύ τους (π.χ. βασικά χαρακτηριστικά, μέτρα ασφάλειας συστήματος και κατάσταση προφύλαξης κάθε μιας πληροφορίας).
- **Μοντέλα φίλτρου**. Υπάρχει μια σύνδεση ανάμεσα στο μοντέλο του καταλόγου και σε αυτό του πίνακα.
- **Μοντέλα επαλλήλων στρωμάτων**. Υπάρχουν επίπεδα για να αντιμετωπίζονται τα θέματα ασφαλείας ξεχωριστά και διαφορετικά από στάδιο σε στάδιο. Το κάθε ένα στάδιο από αυτά προορίζει τους στόχους και τους προορισμούς.

1.8) Απώλειες σε ένα Πληροφοριακό Σύστημα

Ορισμένες πιθανές απώλειες που υπάρχει περίπτωση να συμβούν σε ένα ΠΣ χωρίζονται σε δύο πολύ απλές πράξεις, τις ηθελημένες και τις αθέλητες. Στις ηθελημένες για παράδειγμα ένας μη εξουσιοδοτημένος χρήστης γνωρίζει τη διαδρομή των πράξεών του ως το τελικό αποτέλεσμα, ενώ στις αθέλητες το πρόσωπο αυτό δε γνωρίζει τη διαδρομή των ενεργειών του. Με βάση τις δύο παραπάνω πράξεις, οι απώλειες ταξινομούνται σε τρεις κατηγορίες, την *αδυναμία χρήσης ηλεκτρονικού υπολογιστή*, την *απώλεια χρημάτων* και την *απώλεια αποκλειστικής χρήσης*.

1. Αδυναμία χρήσης Η/Υ. Στην περίπτωση που ο υπολογιστής είναι εκτός λειτουργίας, οι υπηρεσίες που παρέχει είναι υπό διακοπή και αυτό οφείλεται στα εξής:
    - Αδυναμία σύνδεσης με τον κεντρικό Η/Υ. Αυτό μάλλον οφείλεται στην υψηλή φόρτωση των τηλεπικοινωνιακών δικτύων λόγω της αναξιοπιστίας του δικτύου ώστε να μπορεί να φιλοξενεί ταυτόχρονα μεγάλο πλήθος χρηστών σε περιπτώσεις ανάγκης.
    - Εξαιτίας διακοπής ηλεκτρικού ρεύματος. Αυτό για να αντιμετωπιστεί μπορεί να πραγματοποιηθεί με γεννήτριες παροχής ηλεκτρικού ρεύματος που συνδέονται αυτομάτως στο δίκτυο όταν είναι αναγκαίο, τα λεγόμενα UPS (Uninterrupted Power Supply).
    - Πρόβλημα λογισμικού. Αυτό οφείλεται κυρίως σε ανθρώπινα σφάλματα με έλλειψη γνώσεως από τον χρήστη και αντιμετωπίζεται με την εγγύηση διαρκής και σωστής λειτουργίας.
    - Πρόβλημα υλικού. Και αυτό οφείλεται όπως το πρόβλημα του λογισμικού, εξαιτίας ανθρώπινων σφαλμάτων και ελλιπής συντήρησης.

2. Απώλεια χρημάτων. Στην περίπτωση που το ΠΣ είτε καταστραφεί, είτε υποβαθμιστεί, τότε νοείται η απώλεια χρημάτων και αυτό εμφανίζεται είτε μέσω χρήσης υπολογιστή για έργο αλλιώτικο από αυτό που έχει ανατεθεί, είτε με την υποκλοπή του υπολογιστή όταν πρόκειται για μεγάλα συστήματα.

3. Απώλεια αποκλειστικής χρήσης. Στην περίπτωση που ένας μη εξουσιοδοτημένος χρήστης έχει τη δυνατότητα να χρησιμοποιήσει το ΠΣ, τότε χάνεται η αποκλειστικότητα της χρήσης.

1.9) Ασφάλεια & Προστασία των ΠΣ ως Κοινωνική Υπόθεση

Στις μέρες μας, η ύπαρξη μέτρων ασφαλείας σε ένα ΠΣ δεν είναι επωφελή μόνο στους ιδιοκτήτες του και στους σχεδιαστές του. Πολλοί είναι αυτοί που ισχυρίζονται κάτι αντίθετο, όμως σήμερα, το ΠΣ υποδύεται σπουδαίο ρόλο μέσα στο όλο σύστημα και το οποίο ΠΣ μπορεί να είναι είτε μια επιχείρηση, είτε οποιοσδήποτε φορέας, οπότε αυξάνονται και αυτοί που επωφελούνται από την ασφάλεια και την προστασία. Έτσι αποκτάν κατά κάποιον τρόπο δικαίωμα απαίτησης ώστε το ΠΣ τους να ικανοποιείται από συγκεκριμένους κανόνες ασφάλειας και προστασίας.

Όσοι επιθυμούν και επιδιώκουν την ύπαρξη μηχανισμών και μέτρων ασφαλείας είναι οι εξής:

- Ιδιοκτήτης, ο οποίος επιθυμεί να αποφύγει κάθε εμπόδιο που στρέφεται κόντρα στη λειτουργία του ΠΣ της επιχείρησής του γιατί γνωρίζει πως απαιτούνται αρκετά έξοδα για τη δημιουργία ενός τέτοιου συστήματος.
- Πελάτης, ο οποίος πρέπει να έχει γνώση των πραγμάτων διότι κυρίως εξαρτάται από την ορθή και ασφαλή λειτουργία του συστήματος που χρησιμοποιεί.
- Σχεδιαστής, ο οποίος καλείται να ικανοποιήσει τις απαιτήσεις που του έχει υποβάλλει ο αναλυτής για λογαριασμό του ιδιοκτήτη ή του οποιουδήποτε χρήστη.
- Χρήστης, ο οποίος επιθυμεί να μη βρίσκουν εμπόδιο οι λειτουργίες του συστήματος από οποιαδήποτε παρεμβολή.

1.10) Πολιτική Αντιγράφων Ασφαλείας

Για την πιο αποτελεσματική προστασία των αρχείων και δεδομένων, δημιουργώντας αντίγραφα ασφαλείας αποφεύγουμε την μόνιμη απώλεια τους ή αλλιώτικα την αντικατάσταση (επαναφορά) τους σε περίπτωση αθέλητης διαγραφής. Υπάρχει περίπτωση να συμβούν τα παραπάνω, καθώς και να απειληθούν από ιό, οπότε έχοντας το αντίγραφο ασφαλείας, η επιχείρηση ή ο χρήστης θα είναι σε θέση να επαναφέρει τα δεδομένα που χρειάζεται. Πολλά από τα δεδομένα των συστημάτων που ίσως παραβιαστούν είναι σημαντικά και πρέπει να παραμείνουν απόρρητα, γι' αυτόν το λόγο τα αντίγραφα εξυπηρετούν αυτόν τον σκοπό κατά ένα μεγάλο ποσοστό.

Η πολιτική αντιγράφων ασφαλείας συμφέρει διότι εξασφαλίζει ανάκτηση τηλεπικοινωνιακού εξοπλισμού αμέσως, όταν κριθεί αναγκαίο, μετά από κάποια ζημιά κακόβουλης επίθεσης. Στόχος λοιπόν, είναι να καθορίζει τους κανόνες των αντιγράφων ασφαλείας και τις διαδικασίες που χρειάζονται για την διαγραφή εκτεθειμένων πληροφοριών και ανάκτησης δεδομένων.

Για να αναφερθούμε σε πιο συγκεκριμένα χαρακτηριστικά, η πολιτική αντιγράφων ασφαλείας περιλαμβάνει τις εξής παρακάτω διαδικασίες:

- Ανάλυση των μειονεκτημάτων, δηλαδή τη διαδικασία που χρειάζεται για να προσδιοριστούν οι ευπάθειες των προγραμμάτων που επεξεργάζονται, αποθηκεύουν και μεταδίδουν πληροφορίες και δεδομένα.
- Ανάκτηση των δεδομένων, δηλαδή ένα σχέδιο που θα διατηρεί ακριβή αντίγραφα πληροφοριών, το οποίο θα ενημερώνεται κάθε συγκεκριμένη

χρονική περίοδο που θα ανακτά και θα κρατά απόρρητες και ασφαλείς τις πληροφορίες.

- Αποκατάσταση των δεδομένων, δηλαδή ένα σχέδιο που να επιτρέπει την επαναφορά των στοιχείων από τους κατόχους του συστήματος όταν αυτό βρεθεί σε κατάσταση συναγερμού από κάποια κακόβουλη απειλή.
- Έκτακτη ανάγκη, είναι ένα σχέδιο τρόπου λειτουργίας το οποίο θα βοηθάει στην εξαναγκασμένη εκκίνηση του συστήματος όταν αυτό αποτυγχάνει να ξεκινήσει.
- Έλεγχος των εφεδρικών αντιγράφων, δηλαδή η διαδικασία για το πώς προσδιορίζεται ο τρόπος της δημιουργίας τους.
- Επίπεδα ασφαλείας, δηλαδή τα αντίγραφα ασφαλείας θα πρέπει να διαχωρίζονται από τα αρχικά δεδομένα και να διατηρούνται σε διαφορετικές τοποθεσίες για λόγους ασφαλείας.

1.11) Ερμηνεία Firewall και Ασφάλεια στο Διαδίκτυο

Μια αποτελεσματική λύση για την προστασία στο διαδίκτυο είναι η εγκατάσταση μιας ασφαλούς «πύλης» (gateway) η οποία ονομάζεται firewall και βρίσκεται τοποθετημένη ανάμεσα στο εσωτερικό δίκτυο κάποιας εταιρείας – οργανισμού και στο υπόλοιπο διαδίκτυο (internet). Σε πραγματικό χρόνο, περίπου το 30% των μηχανών που έχουν σύνδεση στο διαδίκτυο βρίσκονται υπό την προστασία των firewalls. Οπότε, οι περισσότερες δικτυακές υπηρεσίες καλούνται να αντιμετωπίσουν περιστάσεις εισόδων και εξόδων από κάποιο εσωτερικό δίκτυο μέσω κάποιου τοπικού τοίχους.

Ο «πύρινος τοίχος» έχει ως στόχο να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση μεταξύ δικτύων, δηλαδή να παρέχει προστασία στο εσωτερικό δίκτυο μιας εγκατάστασης (π.χ. σε έναν ιστότοπο) από το υπόλοιπο διαδίκτυο. Αν η εγκατάσταση αυτή διαθέτει firewall, τότε πρέπει να ληφθούν αποφάσεις για το τι πρόκειται να εισαχθεί πέρα από αυτόν τον τοίχο. Οι αποφάσεις αυτές πρέπει να αναδεικνύονται κατ' ευθείαν από την πολιτική ασφαλείας. Μεγάλη πιθανότητα υπάρχει να περιοριστούν οι διαθέσιμες επιλογές εγκατάστασης των διαδικτυακών υπηρεσιών όπως για παράδειγμα οι γνωστές UDP, HTTP, FTP, DNS κ.α.

Μια από τις βασικές λειτουργιές του firewall που διαρκώς βρίσκεται σε εφαρμογή είναι η εξέταση των IP πακέτων που ταξιδεύουν μεταξύ του internet και του εσωτερικού δικτύου. Η παραπάνω πρόταση είναι μια μέθοδος για να ελέγχεται η ροή των πληροφοριών για κάθε υπηρεσία (service) κατά διεύθυνση IP, θύρα (port) και προς κάθε κατεύθυνση.

Το τοίχος προστασίας υλοποιεί μια πολιτική ασφαλείας με την οποία καθορίζονται οι ισορροπίες ανάμεσα στην διατήρηση της ασφάλειας και στην εύχρηστη διαχείριση. Η αυστηρή πολιτική που υποστηρίζει πως «ότι δεν επιτρέπεται, απαγορεύεται» απαιτεί την ανεξάρτητη ενεργοποίηση κάθε υπηρεσίας. Από την άλλη πλευρά, η πολιτική που υποστηρίζει πως «ότι δεν απαγορεύεται, επιτρέπεται» παίρνει ρίσκο για χάρη της ευκολίας και θυσιάζει ένα μέρος από την προστασία. Αν κάποια ενέργεια δεν είναι επιτρεπτή σύμφωνα με την πολιτική του firewall, τότε οφείλει να διασφαλίζει την αποτυχία κάθε προσπάθειας εκτέλεσης της ενέργειας αυτής. Για παράδειγμα, κάθε ενέργεια του ηλεκτρονικού ταχυδρομείου προς συναλλαγή δεδομένων και πληροφοριών μεταξύ χρηστών, εξετάζεται αν μπορεί να γίνει αποδεκτή σύμφωνα με τις προκαθορισμένες πολιτικές ασφαλείας ώστε να εκτελεστεί η συγκεκριμένη ενέργεια με επιτυχία.

Επιπλέον, ο «πύρινος τοίχος» είναι ένας "μηχανισμός" που απομονώνει και αναλύει τα δεδομένα και τα πακέτα πληροφοριών. Επομένως, είναι ένα σύνολο εξοπλισμού και

λογισμικού το οποίο μπορεί να υλοποιηθεί με αλληλεπιδραστικό τρόπο με τις επόμενες διατάξεις:

- με ένα router (δρομολογητή),
- με έναν server (εξυπηρετητή),
- με τον συνδυασμό routers & servers,
- με τον συνδυασμό routers, servers & δικτύων.

Υποψίες γεγονότων απ' τα οποία εξακριβώθηκαν στοιχεία θα πρέπει να καταχωρούνται σε ένα ειδικά υλοποιημένο αρχείο (.log file). Επιπροσθέτως, πρέπει να υπάρχει ειδοποίηση των διαχειριστών για το ζήτημα της εγκατάστασης για κάθε προσπάθεια εισβολής παρανομών στο εκάστοτε δίκτυο. Κάποια συγκεκριμένα firewalls έχουν την ικανότητα να παρέχουν και στατιστικές μελέτες διακίνησης πληροφοριών, καθώς και διάφορες υπηρεσίες κρυπτογραφήσεως και αποκρυπτογραφήσεως πληροφοριών κατά τις εισόδους και τις εξόδους από το διαδίκτυο αντιστοίχως. Τέλος, ερευνάται η δυνατότητα επανελέγχου των ήδη μεταφερόμενων αρχείων – δεδομένων του ηλεκτρονικού ταχυδρομείου για πιθανή μόλυνση από ιούς, αποθηκεύονται για ένα μικρό χρονικό διάστημα και αποστέλλονται ξανά προς τον τελικό προορισμό τους.

1.12) Antivirus softwares – Λογισμικά προστασίας από ιούς

Τα antivirus, γνωστά και ως anti-malwares, δηλαδή τα λογισμικά προστασίας των υπολογιστών που χρησιμοποιούνται για την πρόληψη, ανίχνευση και αφαίρεση κακόβουλων δεδομένων τα οποία έχουν εισχωρήσει με κάποιον τρόπο στο λειτουργικό σύστημα.

Αρχικώς, τα antivirus αναπτύχθηκαν με σκοπό να αντιμετωπίζουν και να απομακρύνουν τους ιούς των υπολογιστών, όμως με την πάροδο του χρόνου και τη ραγδαία αύξηση του διαδικτύου, τα κακόβουλα λογισμικά πολλαπλασιάστηκαν και έτσι τα λογισμικά προστασίας άρχισαν να παρέχουν εντατικότερη ασφάλεια για όλο το φάσμα των απειλών που υπάρχουν σήμερα. Πιο συγκεκριμένα, ένα σύγχρονο λογισμικό προστασίας μπορεί να προστατεύσει το σύστημα από:

- **Κακόβουλα Browser Helpers Objects (BHO).** Το BHO είναι ένα .dll αρχείο που έχει σχεδιαστεί ως plug-in για τον περιηγητή Internet Explorer ώστε να παρέχει πρόσθετες λειτουργίες. Τα BHOs εισήχθησαν τον Οκτώβριο του 1997, όταν κυκλοφόρησε η τέταρτη έκδοση του Internet Explorer.
- **Browser hijackers.** Οι browser hijackers έχουν να κάνουν με την πειρατεία των browsers. Είναι μια μορφή ανεπιθύμητου λογισμικού που τροποποιεί (δίχως την άδεια του χρήστη) τις ρυθμίσεις του εκάστοτε προγράμματος που χρησιμοποιεί ο χρήστης για την περιήγησή του στο διαδίκτυο. Συνήθως αυτό το λογισμικό εισφέρει ανεπιθύμητα διαφημιστικά μηνύματα.
- **Ransomwares.** Το ransomware είναι ένα είδος κακόβουλου λογισμικού που περιορίζει την πρόσβαση στο μολυσμένο σύστημα του υπολογιστή και απαιτεί από τον χρήστη να καταβάλει χρηματικό ποσό στον φορέα του antivirus για να αφαιρεθεί ο περιορισμός.
- **Keyloggers.** Τα keyloggers αφορούν την καταγραφή της πληκτρολόγησης, δηλαδή τη δράση του χρήστη πάνω στο πληκτρολόγιο καθώς εν άγνοιά του οι ενέργειές του βρίσκονται υπό διαρκή παρακολούθηση.
- **Backdoors.** Στα ελληνικά μεταφράζεται και ως κερκόπορτα, η οποία στην πληροφορική θεωρείται ως μια μυστική μέθοδος που παρακάμπτει την

πραγματική ταυτότητα ενός προϊόντος, υπολογιστικού συστήματος, κρυπτοσυστήματος ή αλγόριθμου. Οι πίσω πόρτες χρησιμοποιούνται συχνά για την εξασφάλιση μη εξουσιοδοτημένη απομακρυσμένης πρόσβασης σε έναν υπολογιστή ή την απόκτηση πρόσβασης σε ένα απλό κείμενο στα κρυπτογραφικά συστήματα.

- **Rootkits.** Από τους όρους root (δηλαδή το γνωστό όνομα του admin σε λογισμικά Unix) και kit (δηλαδή το συστατικό στοιχείο του λογισμικού που εφαρμόζουν το εργαλείο). Άρα rootkit είναι μία συλλογή λογισμικού που έχει σχεδιαστεί για να επιτρέπει την πρόσβαση σε έναν υπολογιστή εφόσον δεν επιτρέπεται λόγω μη εξουσιοδοτημένου χρήστη αφού ταυτόχρονα καμουφλάρεται η ύπαρξή του από άλλο λογισμικό.
- **Trojan horses.** Οι γνωστοί δούρειοι ίπποι της πληροφορικής, κακόβουλα προγράμματα που παραποιούνται μόνα τους για να φανούν χρήσιμα και ενδιαφέροντα προς το χρήστη, προκειμένου αυτός να πειστεί και να τα εγκαταστήσει.
- **Worms.** Τα γνωστά σκουλήκια της πληροφορικής, τα οποία αναπαράγονται και εξαπλώνονται μέσα σε ένα δίκτυο υπολογιστών ώστε να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.
- **Κακόβουλα LSPs (Layered Service Providers).** Η LSP (πολυεπίπεδη πάροχος υπηρεσιών) είναι ένα αρχείο .dll το οποίο χρησιμοποιεί winsock API (τεχνική προδιαγραφής που ορίζει τον τρόπο που το λογισμικό των windows θα πρέπει να έχει πρόσβαση στο διαδίκτυο) ώστε να προσπαθήσει να εισαχθεί το ίδιο μέσα στο TCP/IP πρωτόκολλο. Έτσι, εάν το αρχείο .dll είναι μολυσμένο, μπορεί να προκαλέσει φθορές στα πρωτόκολλα διαδικτυακές πρόσβασης του συστήματος.
- **Fraudtools.** Το rogue security software είναι μια μορφή κακόβουλου λογισμικού για την απάτη στο διαδίκτυο το οποίο παραπλανά τους χρήστες ώστε να πιστέψουν πως υπάρχει ένας ιός στον υπολογιστή τους. Το παραπάνω λογισμικό τους προτείνει να καταβάλουν κάποια χρήματα ώστε να αντιμετωπιστεί η συγκεκριμένη δήθεν απειλή που στην ουσία η απειλή βρίσκεται στο ίδιο το κακόβουλο λογισμικό. Αυτό είναι μία μορφή scareware η οποία χειραγωγεί τους χρήστες, τους εκφοβίζει μέσω του ransomware[2] τρόπου.
- **Adwares.** Είναι διαφημίσεις που υποστηρίζονται από κάποιο λογισμικό πακέτο που καθιστά αυτόματα διαφημίσεις προκειμένου να δημιουργηθούν έσοδα για το συγγραφέα του πακέτου.
- **Spywares.** Είναι λογισμικά που έχουν ως στόχο να συγκεντρώνουν πληροφορίες για ένα πρόσωπο ή οργανισμό εν άγνοιά τους. Τα συγκεκριμένα λογισμικά έχουν τη δυνατότητα να στέλνουν τις πληροφορίες αυτές σε άλλο φορέα χωρίς την έγκριση του χρήστη.

Ορισμένα antivirus περιλαμβάνουν προστασία και σε άλλες απειλές που ενδέχεται να μολύνουν ένα σύστημα, μία από αυτές είναι και τα κακόβουλα URLs (links – σύνδεσμοι). Επίσης:

- Το spamming, το οποίο αφορά τη χρήση των ηλεκτρονικών συστημάτων ανταλλαγής μηνυμάτων για την αποστολή ανεπιθύμητων μηνυμάτων,

[2] Ransomware είναι μορφές κακόβουλων λογισμικών που περιορίζουν την πρόσβαση στο μολυσμένο σύστημα του υπολογιστή με κάποιον τρόπο και απαιτούν από τους χρήστες να καταβάλουν λύτρα στους malware φορείς ώστε να αφαιρεθεί ο περιορισμός.

ιδιαιτέρως διαφημιστικών, όμως η σημαντικότερη χρήση του έχει να κάνει με την επαναλαμβανόμενη αποστολή μηνυμάτων αδιάκοπα ανά τακτά χρονικά διαστήματα στον ίδιο χώρο.

- Το scamming, το οποίο έχει να κάνει με ένα τέχνασμα εμπιστοσύνης, δηλαδή μία προσπάθεια ώστε να εξαπατηθεί ένα πρόσωπο ή μια ομάδα ατόμων. Συνήθως, οι συγκεκριμένοι απατεώνες (λογισμικά), εκμεταλλεύονται μερικά χαρακτηριστικά της ανθρώπινης ψυχής όπως ειλικρίνεια, συμπόνια, απληστία, ματαιοδοξία, ευθύνη, ανευθυνότητα, ώστε να πείσουν τους χρήστες να πέσουν στην παγίδα.
- Το phising είναι η προσπάθεια ενός κακόβουλου χρήστη ή λογισμικού, να αποκτήσει ευαίσθητες πληροφορίες (π.χ. ονόματα χρηστών, κωδικούς πρόσβασης κ.α.). Το ηλεκτρονικό ψάρεμα γίνεται συχνά από μεταμφιέσεις κάποιων κακόβουλων χρηστών ως αξιόπιστων προσώπων μέσα σε μια ηλεκτρονική επαφή – επικοινωνία.
- Οι botnet DDoS είναι επιθέσεις που προκαλούν φθορές στους πόρους του δικτύου ή του υπολογιστή ώστε να μην είναι διαθέσιμοι για τους χρήστες, που προσωρινά ή επ' αόριστον θα διακοπούν οι εκάστοτε υπηρεσίες.

Ωστόσο, οι επαγγελματικές εκδόσεις των anti-malwares παρέχουν περισσότερα μέτρα στην ασφάλεια και προστασία σε παγκόσμια κλάση. Επίσης, παρέχεται banking προστασία για ασφαλής ηλεκτρονικές αγορές και πληρωμές μέσω ενός απόλυτα προστατευμένου προγράμματος περιήγησης. Συνεχώς σαρώνει όλες τις εφαρμογές, τα αρχεία και τις συσκευές που συνδέονται στον υπολογιστή για τυχόν απειλές που προσπαθήσουν να εισβάλλουν στο σύστημα

1.13) Επίπεδα Προστασίας των ΠΣ

Με βάση όσων έχουμε αναφέρει μέχρι στιγμής, έχει γίνει κατανοητή η σημασία των ΠΣ μέσα στη ζωή σήμερα καθώς και η αναγκαία προστασία τους από κάθε είδους απειλή. Για να κατηγοριοποιήσουμε την προστασία και την ασφάλεια ώστε να μπορούμε να παρακολουθούμε τις αδυναμίες και να βρίσκουμε λύσεις αποφυγής απωλειών, είναι εφικτό να δημιουργήσουμε ορισμένα επίπεδα. Τα συγκεκριμένα επίπεδα ακούνε στον αριθμό τέσσερα και είναι τα εξής:

1. Φυσική ασφάλεια ενός ΠΣ.
2. Ασφάλεια λειτουργικών συστημάτων.
3. Ασφάλεια δικτύων υπολογιστικών συστημάτων.
4. Ασφάλεια συστημάτων βάσεων δεδομένων.

Παρακάτω θα αναφέρουμε μερικές πληροφορίες σχετικές για κάθε ένα από τα προαναφερθέντα επίπεδα.

1. **Φυσική ασφάλεια του ΠΣ.** Για τη φυσική ασφάλεια καταλαβαίνουμε ότι εννοείται η αντιμετώπιση δυσμενής συνθηκών όπως πυρκαγιές, πλημμύρες, σεισμοί και διάφορα άλλα φυσικά φαινόμενα. Για την ορθή αντιμετώπιση και αποφυγή αυτών, βασιζόμαστε στον κατάλληλο σχεδιασμό του κτηρίου, στη σωστή εκπαίδευση του προσωπικού και την παροχή μηχανισμών ασφαλείας, όπως για παράδειγμα των εξοπλισμό πυρόσβεσης. Αναγκαίο καθήκον είναι και η συστηματική συντήρηση των ηλεκτρικών εγκαταστάσεων. Επίσης,

χρήσιμη φαίνεται να είναι και η ύπαρξη γεννήτριας για την παροχή ηλεκτρικής ενέργειας ή το γνωστό σύστημα ασταμάτητης παροχής τάσεως (UPS), ώστε να αποφεύγονται απώλειες κατά τη διάρκεια πτώσης της τάσης του ηλεκτρικού ρεύματος. Όμως, τα περισσότερα από τα παραπάνω παραλείπονται για οικονομικούς λόγους.

2. **Ασφάλεια λειτουργικών συστημάτων.** Το σημαντικότερο σημείο ενός ΠΣ είναι το λειτουργικό σύστημα (operating system). Λειτουργικό σύστημα ενός υπολογιστή ορίζεται το προϊόν λογισμικού που ελέγχει τα ήδη εκτελεσμένα προγράμματα και παρέχει διάφορες υπηρεσίες όπως τη διαχείριση μνήμης, ελέγχου εισόδου-εξόδου, μεταγλώττισης, σφαλματοθυρίας, χρονοδρομολόγησης κ.α. Κάποιες από τις ιδιότητες των ΛΣ είναι οι ακόλουθες: *αδιαφάνεια, ακεραιότητα, αξιοπιστία, αποδοτικότητα, ασφάλεια, γενικότητα, διαθεσιμότητα, ευελιξία, ευκινησία, επεκτασιμότητα, ευχρηστία, συντηρησιμότητα*. Σύμφωνα με τις παραπάνω ιδιότητες αντιλαμβανόμαστε ότι το ΛΣ αποτελεί το Α και το Ω της σχεδίασης και της ασφαλούς λειτουργίας κάθε ΠΣ. Οποιαδήποτε ‘‘παράνομη’’ παρέμβαση στο ΛΣ ενδέχεται να φανεί επιβλαβής προκαλώντας σοβαρές συνέπειες και φθορές στη λειτουργία του ΠΣ όπως είναι *η υποβάθμιση λειτουργίας του συστήματος προσωρινά ή και μόνιμα*, *η είσοδος μη εξουσιοδοτημένων χρηστών για την τροποποίηση δεδομένων* κ.α.
3. **Ασφάλεια δικτύων υπολογιστικών συστημάτων.** Ο συγκεκριμένος τομέας έχει σχέση με τις ικανότητες που διαθέτει ένας οργανισμός ή μια επιχείρηση ώστε να προστατεύει τα δεδομένα και τις πληροφορίες από πιθανούς κινδύνους. Πέρα από αυτό, γίνεται λόγος και για τη δυνατότητα ενός τέτοιου δικτύου να φέρει αξιόπιστη αντίσταση σε απλές καταστάσεις ή ακόμα και σε επικίνδυνες ενέργειες οι οποίες θέτουν σε κίνδυνο την ακεραιότητα του απορρήτου των δεδομένων. Επίσης, αυτός ο τομέας συνδέεται στενά με τις τρεις βασικές ιδέες που αναφέραμε αρχικώς στις προϋποθέσεις ασφάλειας ενός ΠΣ.
4. **Ασφάλεια συστημάτων βάσεων δεδομένων.** Η πληροφορία είναι η ‘‘περιουσία’’ των ΠΣ, γι’ αυτό έχει μεγάλη αξία και γι’ αυτό η ασφάλεια βάσεων δεδομένων αποκτά μεγάλη σημασία εφόσον οι οποίες αποθηκεύουν, επεξεργάζονται και μεταδίδουν τις πληροφορίες. Η αξιοπιστία της μετάδοσης ελέγχεται από ειδικά πρωτόκολλα τα οποία εγγυώνται την αποτελεσματική και ορθή ολοκλήρωση μεταφορών των πληροφοριών και εφαρμόζουν κανόνες ακεραιότητας. Επίσης, η διαθεσιμότητα για τους χρήστες που κατέχουν δικαιώματα εξουσιοδότησης είναι απαραίτητη και αναγκαία. Οι βασικές διαστάσεις παραμέτρων ασφάλειας ΒΔ ακούνε στα ονόματα *ακεραιότητα, διαθεσιμότητα, έλεγχος προσπέλασης, εμπιστευτικότητα* κ.α., ενώ οι νέες διαστάσεις παραμέτρων ακούνε στα ονόματα *διακριτότητα, έμμεση προσπέλαση, καταγραφή, συνάθροιση, φιλτράρισμα* κ.α.

1.14) Ανάλυση Επικινδυνότητας (Risk Analysis)

Η αξιολόγηση της ασφάλειας των πληροφοριακών συστημάτων μπορεί να αναλυθεί με ποικίλους τρόπους ώστε να διαμορφωθεί μία αξιόπιστη πολιτική ασφαλείας. Για να γίνει πιο κατανοητό θα εκφράσουμε κάποιους ορισμούς που είναι αρκετά γνωστοί για την ανάλυση των κινδύνων:

- Αντίμετρο είναι ένα μέτρο το οποίο λαμβάνεται για την προστασία του ΠΣ και την αντιμετώπιση των απειλών. Ενεργώντας με ανιχνευτικό τρόπο, μειώνοντας την απώλεια που ενδέχεται να προέλθει όταν θα εμφανιστούν κάποιες απειλές.

- Απειλή είναι ένα ανεπιθύμητο γεγονός που έχει την ικανότητα να προσφέρει βλάβες στις υπηρεσίες ενός ΠΣ, τυχαία ή συγκεκριμένα με πρόθεση να καταστρέψει δεδομένα ή/και ολόκληρο το ίδιο το σύστημα καθώς και να κλέψει σημαντικές πληροφορίες δίχως να κατέχει εξουσιοδοτημένη άδεια χρήσης.

- Ευπάθεια είναι μια αδυναμία του συστήματος, συνήθως λανθασμένης σχεδίασης των υποδομών του με αποτέλεσμα να μην είναι σε θέση να λειτουργεί εκατό τοις εκατό σωστά, διατρέχοντας έτσι σε κίνδυνο την παραβίαση της ασφάλειας και ακεραιότητας του ΠΣ.

- Κίνδυνος είναι η πιθανότητα επιτυχίας μια συγκεκριμένης απειλής να εκμεταλλευτεί την ευπάθεια του συστήματος και έτσι να υπάρχουν ενδεχόμενα για απώλειες.

Οφέλη

Μετά από την ανάλυση επικινδυνότητας μπορούμε να αποκομίσουμε μερικά οφέλη τα οποία είναι:

1. Βελτίωση της ασφάλειας πληροφοριακών συστημάτων.
2. Βελτίωση στην κατανόηση του συστήματος.
3. Δικαιολόγηση για τις δαπάνες της ασφάλειας.
4. Κατανόηση για την ανάγκη της ασφάλειας.

Μέθοδοι

Για να αξιολογήσουμε τα επίπεδα ασφαλείας των πληροφοριακών συστημάτων μπορούμε να εφαρμόσουμε κάποιες μεθόδους (τεχνικές) ανάλυσης επικινδυνότητας. Αυτές που έχουν αρκετά διαδοθεί ευρέως είναι οι SBA (Security By Analysis), η Marion και η CRAMM (CCTA Risk Analysis and Management Method).

Η πολιτική ασφάλειας θα διαμορφωθεί με τα αποτελέσματα της ανάλυσης επικινδυνότητας. Άξια πλεονεκτήματα για την ανταπόκριση σημαντικών αναγκών, για την πολιτική ασφαλείας στην μελέτη της επικινδυνότητας και στο επίπεδο της παρεχόμενης ασφάλειας, για τον οργανισμό με την ανάλογη επιλογή των μέτρων προστασίας που τα ΠΣ αντιμετωπίζουν τους κινδύνους. Από την άλλη, το μειονέκτημα που υπάρχει αφορά σε προσωπικό και υποκειμενικό επίπεδο την κρίση του αναλυτή και το πώς αυτός θα χρησιμοποιήσει σωστά τις μεθόδους με τη γνώση και την εμπειρία του.

Τύπος BPL

Υπάρχει ένας τύπος που μπορεί να αναλυθεί μέσα από αυτόν ο κίνδυνος. Ο τύπος είναι ο **B > P * L** και συνήθως υπολογίζει την πιο συμφέρουσα λύση. Όμως η εφαρμογή του τύπου και ο υπολογισμός της πρακτικής του συναντά κάποιες δυσκολίες. Τα τρία στοιχεία του τύπου είναι:

B = Κόστος για την πρόληψη μιας απώλειας
P = Ενδεχόμενο να συμβεί μια απώλεια
L = Συνολικό κόστος μιας απώλειας

Το νόημα του παραπάνω τύπου αντικατοπτρίζει το κόστος της πρόληψης μιας απώλειας (B), το οποίο είναι μεγαλύτερο (>) από το γινόμενο της πιθανότητας να συμβεί μια απώλεια (P), επί (*) του συνολικού κόστους της απώλειας (L). Αν συμβεί το παραπάνω τότε κρίνεται ως υπερβολικό το μέτρο πρόληψης, όμως εάν συμβεί το αντίθετο τότε μας συμφέρει να υλοποιήσουμε αυτό το μέτρο.

Μέτρα Ασφαλείας

Τα μέτρα ασφαλείας – προστασίας αφορούν όλες τις ενέργειες και τις διαδικασίες που περιορίζουν τις απειλές και τους κινδύνους ενός ΠΣ, τα οποία διακρίνονται στις τέσσερις εξής παρακάτω κατηγορίες:

- Πρόληψη: τα μέτρα αυτά καταβάλλουν προσπάθειες για τη μείωση των κινδύνων.
- Διασφάλιση: εργαλεία και στρατηγικές που βοηθούν στη διαρκής εξασφάλιση και συνεχής αποτελεσματικότητας των συγκεκριμένων μέτρων.
- Ανίχνευση: συγκεκριμένα προγράμματα και τεχνικές που βοηθούν στην αντιμετώπιση ανεπιθύμητων περιστατικών.
- Επαναφορά: διαδικασίες που έχουν στόχο τη γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον εφόσον υπήρξε παραβίαση ασφάλειας και ταυτόχρονα έρευνα για την αιτία που την προκάλεσε.

Για να υπάρχει επιτυχία στην πολιτική της ασφαλείας, στο πλάνο της ασφαλείας οφείλεται να περιλαμβάνεται και η διαδικασία ενημέρωσης (update) ώστε με επισκοπήσεις της εφαρμογής να υπάρχει πάντα σε διαθεσιμότητα το up-to-date αναλόγως με τις τεχνολογικές εξελίξεις και αλλαγές της εταιρίας του αντίστοιχου λογισμικού.

Απαιτήσεις Ασφαλείας

Στην Ασφάλεια Πληροφοριακών Συστημάτων υπάρχουν κάποιες θεμελιώδης αρχές λειτουργίας που θα πρέπει να ικανοποιούν τις εξής παρακάτω απαιτήσεις ασφαλείας:

1. Η σωστή ανάπτυξη και λειτουργία για να υφίσταται αποδοτική σε ένα ΠΣ πρέπει να εμπεριέχει μια καλή δόμηση ενός πλαισίου ασφαλείας απ' το οποίο να έχουν εξασφαλιστεί όλες προαπαιτούμενες απαιτήσεις για να διατηρηθεί ανέπαφη η μυστικότητα των πληροφοριών και των δεδομένων.
2. Το συνολικό αποτέλεσμα του συστήματος δεν πρέπει να επηρεάζεται από τους μηχανισμούς ασφαλείας. Σε περίπτωση που δεν επιτρέπεται σε κάποιον ενδιαφερόμενο η άδεια για προώθηση σημαντικών και μυστικών πληροφοριών προς τρίτους, θα πρέπει να υπάρχει χρυσή τομή μεταξύ της ασφάλειας και της απόδοσης του συστήματος.
3. Όσο για τα δικαιώματα πρόσβασης εκ των οποίων πρέπει να είναι ανεξάρτητα από τη διαδικασία που χρειάζεται για να υλοποιηθεί ένα ΠΣ, όταν ξεκινήσει η διαδικασία καθορισμού των δικαιωμάτων αυτών, πρέπει να γίνει μέσω δομικών, νομοθετικών και οργανωτικών επιπέδων.
4. Η σωστή διαχείριση των πληροφοριών πρέπει να γίνεται μέσω του κατάλληλου εξουσιοδοτημένου προσωπικού καθώς αυτές να διαχειρίζονται ξεχωριστά από το υπόλοιπο σύστημα.

1.15) Πολιτική Προστασίας – Μηχανισμοί Ασφαλείας

Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ)

Η γενική αρχή του ΑΔΑΕ έχει σκοπό την προστασία του απορρήτου των πληροφοριών που ταξιδεύουν μέσα στα δίκτυα. Μέσα σε αυτήν την έννοια υπάρχει και ο έλεγχος της τήρησης της γενικής αρχής και της διαδικασίας άρσης του απορρήτου που προβλέπεται από τον νόμο.

Στην πράξη η ασφάλεια βρίσκεται στην συνεχή προστασία ανθρώπων και αγαθών που για τα οποία λαμβάνονται μέτρα αποφυγής πιθανών κινδύνων. Παραδείγματος χάριν, για να προστατεύσουμε ένα αυτοκίνητο από απειλές όπως κλοπή, εσκεμμένες φθορές, φυσικές φθορές κ.α., μπορούμε να το προφυλάξουμε με τη βοήθεια μια αποθήκης (γκαράζ), ούτως ώστε να αποτρέψουμε την εισβολή απειλών. Με βάση το παραπάνω παράδειγμα, για να ασφαλίσουμε μια ηλεκτρονική βάση δεδομένων πρέπει να προστατεύσουμε εμείς οι ίδιοι τα δεδομένα από πιθανές καταστροφές που μπορούν να πραγματοποιήσουν μη εξουσιοδοτημένα πρόσωπα.

Η ΑΔΑΕ καθορίζει κάποιες συγκεκριμένες διαδικασίες τεκμηρίωσης, εφαρμογής και αναθεώρησης ασφάλειας. Επίσης, ορίζει κάποιες ενέργειες που αφορά πρόσωπα όπως εργαζόμενους και συνεργάτες, χρήστες και συνδρομητές, πρόσωπα που ασχολούνται με την παροχή δικτύων – υπηρεσιών και γενικώς οποιοσδήποτε είναι υπεύθυνος για οποιαδήποτε ενέργεια που αφορά προστασία συστημάτων.

Ασφαλή μεταφορά δεδομένων μέσω διαδικτύου

I. Για να διασφαλιστούν οι εφαρμογές του διαδικτύου και να εξασφαλιστεί το απόρρητο, υπάρχουν κάποια ανεπτυγμένα πρωτόκολλα που βασίζονται πάνω σε κάποιες γενικές αρχές κρυπτογράφησης, αναλόγως τον τύπο της διαδικτυακής εφαρμογής προσαρμόζονται και τα ανάλογα πρωτόκολλα.
II. Οι διαδικτυακές υπηρεσίες πρέπει να χρησιμοποιούν κάποιες τεχνικές που είναι ευρέως γνωστές και αποδεκτές για την ασφάλεια στο διαδίκτυο. Για παράδειγμα, στις εφαρμογές που αφορούν παγκόσμιους ιστούς (www) πρέπει να υπάρχει το πρωτόκολλο γνωστό ως SSL (Secure Sockets Layer). Επίσης, για τις εφαρμογές ηλεκτρονικού ταχυδρομείου (e-mail) πρέπει να υπάρχει το S/MIME (Secure / Multipurpose Internet Mail Extensions), το PEM (Privacy Enhanced Mail) και το PGP (Pretty Good Privacy). Ωστόσο για πληρωμές μέσω διαδικτύου με τη βοήθεια πιστωτικών καρτών, πρέπει η εφαρμογή να υποστηρίζει το πρωτόκολλο SET (Secure Electronic Transaction).
III. Με την πάροδο των χρόνων και την εξέλιξη της τεχνολογικής επιστήμης τα νέα πρωτόκολλα θα πρέπει να συμβαδίζουν προοδευτικά. Η ΑΔΑΕ είναι υπεύθυνη για νέες οδηγίες προς τους παρόχους διαδικτύου σε ότι έχει να κάνει με τις νέες εξελίξεις των πρωτοκόλλων. Επίσης, οι πάροχοι διαδικτύου οφείλουν να ακολουθούν τα γνωστά πρωτόκολλα με αυστηρά βήματα και οδηγίες από την ΑΔΑΕ.

Πλαίσιο χρήσης μηχανισμών ασφαλείας στο διαδίκτυο

Για μια άκρως υλοποιημένη επικοινωνία μέσω του διαδικτύου πρέπει να περιλαμβάνονται ορισμένα βασικά στοιχεία μεθόδων κρυπτογραφήσεως (encryption), προσδιορισμού ταυτότητας (authentication) από τους χρήστες και κάποιο πλάνο που να διαχειρίζεται τις αποδοτικές μεθόδους κλειδιών και κωδικών πρόσβασης. Όμως πολλές είναι οι φορές που οι κωδικοί πρόσβασης δεν είναι αρκετοί στο να προστατεύσουν και έτσι πρέπει να βοηθήσει ένα άλλο είδος προς την ενίσχυση της πιστοποίησης δεδομένων. Το τελευταίο τείνει προς την επιτυχία με μια ακολουθία διαφορετικών τεχνολογιών, ένα παράδειγμα είναι αυτό με τις γεννήτριες δυναμικών κωδικών, με τεχνικές που βασίζονται στην κρυπτογραφία, στην ψηφιακή υπογραφή και στα πιστοποιητικά.

Επιπροσθέτως, ο πάροχος του διαδικτύου οφείλει να παρέχει προστασία στους διακομιστές του δικτύου του καθώς και να δίνει τη δυνατότητα της ανάκτησης των αρχείων του σε περίπτωση που βρεθεί σε κατάσταση κάποιας απρόοπτης ενέργειας. Οι διαχειριστές δικτύου, από τη δικιά τους πλευρά, οφείλουν να παρέχουν αποτελεσματικούς μεθόδους αντιγράφων όπως για παράδειγμα αυξητικής, διαφορικής και πλήρης αντιγραφής αρχείων. Ακόμα μία μέθοδος η οποία ονομάζεται δικτυακή αντιγραφή αρχείων που τα κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε κάποιο μέρος πέρα από το εσωτερικό δίκτυο του διαδικτυακού παρόχου. Επίσης, είναι ανάγκη να χρησιμοποιηθούν λογισμικά που έχουν την ικανότητα να καταπολεμήσουν τις κακόβουλες επιθέσεις και αυτό επιτυγχάνεται κατά ένα μεγάλο ποσοστό με τη χρήση τοίχων ασφαλείας, τα γνωστά σε πολλούς firewalls, τα οποία προστατεύουν το σύστημα από ιούς.

Όσο αναφορά τους εξυπηρετητές (servers) που υπάρχουν στις εφαρμογές ηλεκτρονικού ταχυδρομείου, μπορούν να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να ελέγχεται μέσω χρήσης ψηφιακής υπογραφής του αποστολέα, μπορούν να αποκλείουν την αποστολή μηνυμάτων σε δέκτες οι οποίοι φαίνονται ακατάλληλοι και επικίνδυνοι καθώς και μπορούν να ανιχνεύουν τα σωστά προγράμματα για αποστολή και λήψη μηνυμάτων. Οι κανόνες ασφαλείας πρέπει να είναι κατανοητοί από όλους τους χρήστες όπως ορίζει ο πάροχος διαδικτύου και να μην τους παραβαίνουν με ανάρμοστους τρόπους σε παράνομους ηλεκτρονικούς τόπους δημοσιοποιώντας υλικό το οποίο είναι σημαντικό και περιέχει απόρρητες πληροφορίες.

Παρακάτω θα περιγράψουμε τους μεθόδους κρυπτογράφησης (encryption), προσδιορισμού ταυτότητας (authentication) και προστασίας από ιούς.

Κρυπτογράφηση (encryption) είναι η επιστήμη που μέσω των μαθηματικών κωδικοποιεί και αποκωδικοποιεί τα δεδομένα. Από τις μεθόδους της, οι ευαίσθητες πληροφορίες είναι προσβάσιμες μόνο από πρόσωπα τα οποία είναι πλήρως εξουσιοδοτημένα. Έτσι στοχεύουν στην εξασφάλιση του απορρήτου όσο αναφορά την ψηφιακή επικοινωνία και στην αποθήκευση ευάλωτων πληροφοριών. Στο διαδίκτυο, η κρυπτογραφία σκοπεύει στην διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη αποποίησης ευθύνης της ιδιωτικότητας του χρήστη για όσο το δυνατόν προστατευμένες συναλλαγές. Ωστόσο, οι πάροχοι δικτύων πρέπει να τείνουν σε διαρκή εφαρμογή διάφορες τεχνικές κρυπτογραφίας σε συστήματα και σε εφαρμογές τους καθώς και στη μετάδοση δεδομένων, με βάση ορισμένα πρότυπα. Επίσης, υποχρέωση των παροχών δικτύων είναι να ενημερώνουν την ΑΔΑΕ για τις τεχνικές τους. Από την άλλη πλευρά, η ΑΔΑΕ πρέπει να παρέχει οδηγίες περί τεχνικού τομέα ώστε να καθορίζουν τα κλειδιά στα πεδία κρυπτογραφήσεων. Η κρυπτογράφηση πρέπει να βρίσκεται σε στάδιο ώστε να μην είναι εύκολη η παραβίαση του συστήματος από τον εισβολέα μέσα σε πραγματικό και λογικό χρονικό διάστημα.

Κάποια ονόματα αλγορίθμων κρυπτογράφησης είναι τα ακόλουθα, τα οποία χωρίζονται σε δύο μεγάλες κατηγορίες, σε συμμετρικές και σε ασύμμετρες κρυπτογραφίες:

- Η *συμμετρική* χωρίζεται σε δύο υποκατηγορίες με βάση τον τρόπο κρυπτογράφησης μηνυμάτων:

  - Δέσμης (Block ciphers): 3DES (Data Encryption Standard), AES (Advanced Encryption Standard), 3-Way, Blowfish, CAST, CMEA, DEAL FEAL, GOST, IDEA, Lucifer, MARS, MISTY, New-DES, SQUARE, Skipjack κ.α. Οι συγκεκριμένοι κρυπτογραφικοί αλγόριθμοι σπάνε σε πολλά κομμάτια το αρχικό μήνυμα και κρυπτογραφούν ξεχωριστά κάθε ένα από αυτά τα κομμάτια.

  - Ροής (Stream Ciphers): OPYX, RC4, SEAL κ.α. Οι συγκεκριμένοι αλγόριθμοι ενεργούν αντίθετα από αυτούς των δέσμιων, δηλαδή κρυπτογραφούν μια ροή μηνύματος (stream) δίχως να τη διασπάνε σε τμήματα.

- Η *ασύμμετρη* δε χωρίζεται σε υποκατηγορίες και κάποια από τα ονόματα των αλγορίθμων είναι: RSA, DSA, ECC (Κρυπτογραφία Ελλειπτικών Καμπυλών), πρωτόκολλο Diffie-Hellman, Paillier, πρότυπο και υπογραφή El Gamal.

Μερικά *κρυπτογραφημένα πρωτόκολλα ασφαλείας* που βοηθούν για την ασφάλεια και την προστασία της ιδιωτικής ζωής στο διαδίκτυο είναι τα εξής: SSL (Secure Socket Layer), TLS (Transport Layer Security), IPSec (Secure IP), HTTP-S (Secure HTTP), PGP & S/MIME (Secure e-mail), DNDSEC, SSH κ.α. Τα παραπάνω πρωτόκολλα χωρίζονται σε κάποιες κατηγορίες με βάση τη δουλειά που ασκεί το κάθε ένα.

- Πρωτόκολλα Εφαρμογών: PGP, S/MIME, S-HTTP, HTTPS, SET, KERBEROS.
- Πρωτόκολλα Διακίνησης: SSL, TLS.
- Πρωτόκολλα Δικτύου: VPN, IPSec.
- Πρωτόκολλα Διασύνδεσης Δεδομένων: PPP, RADIUS, TACACS+.

Παρακάτω θα εξηγήσουμε τα πιο σημαντικά και δημοφιλέστερα πρωτόκολλα που αναφέραμε παραπάνω.

- PGP (Pretty Good Privacy). Αναπτύχθηκε από τον Phil Zimmermann, πρόκειται για ένα δημόσιο κλειδί κρυπτοσυστήματος το οποίο διασφαλίζει την εμπιστευτικότητα του κάθε χρήστη στα μηνύματα του ηλεκτρονικού ταχυδρομείου αλλά και γενικώς μέσα στο διαδίκτυο και αυτός είναι ο λόγος που το PGP είναι τόσο ευρέως γνωστό σήμερα.

- S/MIME (Secure/Multipurpose Internet Mail Extension). Επεκτείνει τα πρωτόκολλα πολλαπλών χρήσεων διαδικτυακού ταχυδρομείου (MIME) και προσθέτει ψηφιακές κρυπτογραφημένες υπογραφές. Το MIME πρόκειται για μια τεχνική προδιαγραφή των πρωτοκόλλων επικοινωνίας η οποία περιγράφει τη μεταφορά των πληροφοριών και των πολυμέσων.

- S-HTTP (Secure-Hyper Text Transfer Protocol). Επεκτείνει το πρωτόκολλο HTTP. Όταν αυτό το πρωτόκολλο αρχικώς αναπτύχθηκε για τις ανάγκες μιας ιστοσελίδας πολύ απλής δίχως γραφικό περιβάλλον, εκείνη την εποχή, ήταν δύσκολο για τις end-to-end συναλλαγές κρυπτογράφησης κι έτσι έπρεπε να βελτιωθεί το συγκεκριμένο πρωτόκολλο απ' το κρυπτογραφικό στάδιο έως και το γραφικό, εφόσον έπρεπε να παραμείνουν οι βάσεις που είχαν δημιουργηθεί από τότε.

- HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer). Σχεδιάστηκε αρχικώς από την εταιρεία Netscape. Χρησιμοποιεί την SSL ως υπόστρωμα κάτω από την HTTP στο πεδίο εφαρμογής της. Όταν χρησιμοποιείται το HTTPS, η σύνδεση πραγματοποιείται με διαφορετική θύρα, την 443, αντί την 80 του HTTP στις αλληλεπιδράσεις του με το κατώτερο στρώμα, το TCP/IP.

- SET (Secure Electronic Transactions). Το κρυπτογραφικό αυτό πρωτόκολλο αναπτύχθηκε από μια ομάδα εταιρειών όπου περιλαμβάνονται οι Visa, MasterCard, Microsoft, IBM, RSA, Netscape κ.α. Είναι ένα εξειδικευμένο σύστημα με αρκετά πολύπλοκες προδιαγραφές που περιέχονται σε τρία βιβλία. Το πρώτο ασχολείται με την περιγραφή των επιχειρήσεων, το δεύτερο είναι οδηγός ενός προγραμματιστή και το τρίτο αναφέρει την επίσημη περιγραφή του πρωτοκόλλου. Σε κάθε συναλλαγή, το SET παρέχει υπηρεσίες ταυτοποίησης, εμπιστευτικότητας και ακεραιότητας μηνύματος. Η σύνδεσή του χρησιμοποιεί το δημόσιο κλειδί κρυπτογράφησης και πιστοποιητικά υπογεγραμμένα τα οποία προσδιορίζουν την ταυτότητα των όσων εμπλέκονται σε οποιαδήποτε συναλλαγή ώστε να επιτρέπεται η κάθε ιδιωτική αλληλογραφία ανάμεσά του.

- Kerberos. Το συγκεκριμένο πρωτόκολλο προσδιορισμού ταυτότητας έχει σχεδιαστεί για να επιτρέπει στους χρήστες του δικτύου να επικυρώνουν την ύπαρξή τους μέσα στο σύστημα και η κρυπτογράφηση πραγματοποιείται με τη χρήση μυστικού κλειδιού. Η επικοινωνία μεταξύ κάποιου απλού χρήστη και ενός διακομιστή γίνεται με ασφάλεια αφού και οι δύο έχουν χρησιμοποιήσει το συγκεκριμένο πρωτόκολλο ώστε να αποδείξουν την ταυτότητά τους.

- SSL (Secure Socket Layers). Αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά τη μετάδοση σημαντικών δεδομένων και πληροφοριών στο διαδίκτυο. Μία έκδοση του συγκεκριμένου πρωτοκόλλου η οποία κυκλοφόρησε το 1996, αποτέλεσε βάση ώστε να αναπτυχθεί μετέπειτα το πρωτόκολλο TLS (Transport Layer Security) που πρόκειται να αντικαταστήσει το SSL. Και τα δύο αυτά πρωτόκολλα είναι απολύτως χρήσιμα και ευρέως γνωστά για ηλεκτρονικές αγορές και χρηματικές συναλλαγές στο διαδίκτυο.

Προσδιορισμός ταυτότητας (authentication) αναφέρεται σε αναγνώριση και ταυτοποίηση, πιο συγκεκριμένα σ' αυτούς που πλοηγούνται στο σύστημα, στο οποίο μπορεί να περιβάλλονται κοινοί χρήστες μέχρι και διαχειριστές, προγραμματιστές, τεχνικό προσωπικό κ.α. Συνεπώς, όσοι διαπράττουν πλοήγηση μέσα στο σύστημα είναι αναγκαίο να έχουν ένα μοναδικό αναγνωριστικό χρήστη, το γνωστό user ID. Οπότε, με τη βοήθεια αυτού του ID, γίνεται εφικτός ο εντοπισμός του συγκεκριμένου προσώπου καθώς και με κάθε

δυνατή λεπτομέρεια η οποιαδήποτε δραστηριότητα που διαπράττει μέσα στο πληροφοριακό σύστημα για το οποίο εργάζεται. Σημαντικό για τα user IDs είναι πως τα δικαιώματα του χρήστη παραμένουν απόρρητα και δεν πρέπει σε καμία περίπτωση να είναι εκτεθειμένα. Μια ομάδα χρηστών μπορεί να δουλέψει για συγκεκριμένες εργασίες μέσα στο σύστημα έχοντας το ίδιο αναγνωριστικό μόνο σε σημαντικές καταστάσεις, εφόσον αυτό κρίνεται αναγκαίο και απαραίτητο από τον οργανισμό και εγκριθεί ειδικά εκ της διοικήσεως.

Μια από τις πιο συνηθισμένες διαδικασίες αυθεντικοποίησης για την επιβεβαίωση στοιχείων ενός χρήστη είναι τα συνθηματικά. Τα συνθηματικά βασίζονται σε ένα πλάνο το οποίο πρέπει να είναι τέρας μυστικότητας και γνωστό μόνο για τον συγκεκριμένο χρήστη. Διάφοροι άλλοι μηχανισμοί προσδιορισμού ταυτότητας περιλαμβάνουν κρυπτογραφήσεις με συνδυασμούς και πρωτόκολλα με εξακρίβωση ταυτότητας του χρήστη.

Επίσης, υπάρχουν αντικείμενα, όπως για παράδειγμα οι έξυπνες κάρτες, οι οποίες πρέπει να βρίσκονται υπό κατοχή του χρήστη ώστε να χρησιμοποιούνται για την αυθεντικοποίηση του στο σύστημα. Άλλος ένας τρόπος για αναγνώριση ταυτότητας χρήστη είναι η εξέταση χαρακτηριστικών του χρήστη όπως για παράδειγμα τα δακτυλικά αποτυπώματα και η κόρη του ματιού. Έτσι, καταλήγουμε στο συμπέρασμα ότι όσο το δυνατόν περισσότεροι τρόποι αναγνώρισης και εξακρίβωσης στοιχείων τόσο πιο αποτελεσματική και ισχυρή θα είναι η αυθεντικοποίηση.

Προστασία από ιούς. Το συγκεκριμένο ζήτημα αφορά τον πάροχο δικτύου, ο οποίος θα πρέπει να διαθέτει λογισμικό τέτοιο ώστε να ανταποκρίνεται με τον κατάλληλο δυνατό τρόπο στην προστασία των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες, όπως για παράδειγμα οι υπηρεσίες e-mail οφείλουν να χρησιμοποιούν e-mail scanner.

Επίσης, για να εξετάζονται αυτομάτως όλα τα εισερχόμενα μηνύματα πρέπει να είναι εγκατεστημένη μία μόνιμη μνήμη (resident memory) στα υπολογιστικά συστήματα λογισμικού. Όμως από την άλλη, οι χρήστες οφείλουν να προστατεύονται και να ενημερώνονται από τους παρόχους υπηρεσιών για νέες τεχνικές – οδηγίες για καλύτερη προστασία.

Ωστόσο, για να αποτρέψουμε και να εντοπίσουμε κακόβουλα λογισμικά πρέπει να υλοποιηθεί και ο κατάλληλος μηχανισμός για την σωστή αντιμετώπιση. Η σωστή προστασία απέναντι στα κακόβουλα λογισμικά ξεκινάει πάντα από τη σωστή ενημέρωση των χρηστών περί ασφάλειας δικτύου/οργανισμού/πληροφοριακού συστήματος καθώς και περί δικαιωμάτων διαχείρισης αλλαγών σε ένα τέτοιο σύστημα.

Παρακάτω, θα διατυπώσουμε ορισμένους μηχανισμούς που αφορούν τον έλεγχο για την προστασία δεδομένων και πληροφοριών.

- ✓ Πολιτική που να επιβάλλει νομιμότητα σε χρήσεις λογισμικών με τις κατάλληλες άδειες και απαγορεύει τις χρήσεις μη εξουσιοδοτημένων λογισμικών.
- ✓ Πολιτική προστασίας των ΠΣ από λογισμικά και αρχεία που έχουν τη δυνατότητα να εισέλθουν στο σύστημα μέσω κάποιο μέσον αποθήκευσης ή μέσω εξωτερικού δικτύου.
- ✓ Εγκατάσταση και ενημέρωση των antivirus για διαρκή και συνεπή έλεγχο των προσωπικών υπολογιστών και τους αποθηκευτικούς τους χώρους.
- ✓ Έλεγχος των λογισμικών που χρησιμοποιήθηκαν ή πρόκειται να χρησιμοποιηθούν καθώς και των αρχείων του συστήματος για πιθανές αλλαγές οι οποίες πρέπει να ερευνούνται και να αναφέρονται.
- ✓ Έλεγχος λογισμικών, αρχείων και αποθηκευτικών μέσων προτού χρησιμοποιηθούν ώστε εάν αντιμετωπίζουν ευπάθειες από ιούς να γίνει έγκυρα γνωστό.

- ✓ Έλεγχος εισερχόμενων e-mails για ιούς από εξυπηρετητές, προσωπικούς υπολογιστές κ.α.
- ✓ Εκμάθηση προς τους χρήστες για την αντιμετώπιση ιών και πειραματικές διαδικασίες όταν ένας ιός κάνει την εμφάνισή του.
- ✓ Έτοιμο καταστρωμένο πλάνο σε περίπτωση που ένα σύστημα βρεθεί εκτεθειμένο από φθορές ιών ώστε η επιχείρηση να συνεχίσει δίχως να χάνει χρόνο για την επιδιόρθωση του προβλήματος.

Internet Information Services

Οι Υπηρεσίες Πληροφοριών Διαδικτύου, γνωστές και ως IIS[3] (πρώην Internet Information Server) είναι επεκτάσιμες εξυπηρετητές δικτύων που δημιουργήθηκαν από τη Microsoft για να χρησιμοποιηθούν μαζί με τα Windows NT[4]. Τα IIS υποστηρίζουν HTTP, HTTPS, FTP, FTPS, SMTP και NNTP. Ήταν αναπόσπαστο κομμάτι της NT "οικογένειας" έως την έκδοση των NT 4.0, αλλά μπορεί να είναι απούσα από κάποιες εκδόσεις των Windows, όπως των XP Home Edition.

Μερικά χαρακτηριστικά των IIS, από την έκδοση 6.0 και άνω, που υποστηρίζουν μηχανισμούς ταυτοποίησης είναι τα παρακάτω:

- Ανώνυμος έλεγχος ταυτοποίησης (Anonymous authentication).
- Βασικός έλεγχος ταυτοποίησης (Basic access authentication).
- Έλεγχος ταυτοποίησης Digest[5].
- Ενσωματωμένη ταυτοποίηση των Windows.
- Ταυτοποίηση UNC.
- .NET Passport ταυτοποίησης (αφαιρέθηκε στον Windows Server 2008 και IIS 7.0)
- Πιστοποιητικό ταυτοποίησης (Certificate authentication).

[3] Επίσημη ιστοσελίδα: https://www.iis.net.

[4] Τα Windows NT είναι μία "οικογένεια" λειτουργικών συστημάτων της Microsoft, η οποία κυκλοφόρησε την πρώτη έκδοση NT τον Ιούλιο του '93. Πρόκειται για έναν ανεξάρτητο πολυεπεξεργαστή πολλαπλών χρήσεων. Περισσότερες πληροφορίες εδώ: https://en.wikipedia.org/wiki/Windows_NT.

[5] Πληροφορίες για την Digest ταυτοποίηση εδώ: https://en.wikipedia.org/wiki/Digest_access_authentication.

Στο δεύτερο μέρος της πτυχιακής μας εργασίας αποφασίσαμε να αναφερθούμε στην ανάλυση ασφάλειας ιστοσελίδων, οι οποίες εξυπηρετούν διαδικτυακά καθημερινώς εκατοντάδες ακαδημαϊκούς πολίτες και συναδέλφους μας. Η ανάλυσή μας θα πραγματοποιηθεί με τη βοήθεια μερικών λογισμικών προγραμμάτων, τα οποία θα μας εξυπηρετήσουν στη σάρωση των ιστότοπων του ΤΕΙ Μεσολογγίου, ώστε να ανακαλύψουμε τυχόν κενά ασφαλείας από διάφορες ειδοποιήσεις των χρησιμοποιηθέντων προγραμμάτων.

Όπως θα αναφέρουμε και παρακάτω, μερικούς απ' τους κινδύνους που κυκλοφορούν στο διαδίκτυο και πρέπει να γνωρίζουμε πως υπάρχουν είναι:

1. SQL Injection.
2. Cross Site Scripting (XSS).
3. Man in the Middle.

Υπάρχουν και άλλες απειλές επιθέσεων που απασχολούν το διαδίκτυο, εμείς θα επικεντρωθούμε στις παραπάνω και θα αναφέρουμε κάποια χαρακτηριστικά μέσω μερικών παραδειγμάτων, καθώς θα προσπαθήσουμε να παρακολουθήσουμε μέσω των λογισμικών εάν κάποια από τις παραπάνω επιθέσεις είναι επικίνδυνη για τις ιστοσελίδες του ΤΕΙ Μεσολογγίου.

1.16) SQL Injection

Αρχικώς, η έννοια SQL προέρχεται από τα αρχικά **Structured Query Language** που κατά την ελληνική γλώσσα μεταφράζονται ως "δομημένη γλώσσα ερωτημάτων" (ή αναζήτησης). Οι Βάσεις Δεδομένων στις μέρες μας έχουνε γίνει ένα από τα σημαντικότερα στοιχεία των λειτουργικών συστημάτων διότι μέσα σε αυτές έχουμε την ικανότητα να αποθηκεύσουμε μεγάλο όγκο δεδομένων καθώς και τις ευαίσθητες προσωπικές μας πληροφορίες.

Για να πραγματοποιήσουμε πρόσβαση σε μια ΒΔ μπορούμε να το πετύχουμε μέσω της SQL γλώσσας ώστε *να εκτελούμε ερωτήματα, να αναζητούμε δεδομένα και να εισάγουμε – διαγράφουμε – ενημερώνουμε εγγραφές*.

Όμως, πόσο ασφαλή είναι τα προσωπικά μας στοιχεία τα οποία βρίσκονται κρυμμένα μέσα σε κάποια ΒΔ κάποιας ιστοσελίδας στην οποία έχουμε εγγραφή με όνομα χρήστη, κωδικό και e-mail. Σύμφωνα με δύο λίστες που είχαν δημοσιευτεί το 2010 και 2013 από τον OWASP[6], αναφέρονταν στα 10 πιο επικίνδυνα κενά ασφαλείας σε εφαρμογές διαδικτύου. Τις πρώτες θέσεις και στις δύο αυτές λίστες είχαν καταλάβει οι επιθέσεις τύπου injection και μέσα σε αυτές ανήκει και η γνωστή σε κάποιους επίθεση SQL Injection.

---

[6] Ο OWASP (Open Web Application Security Project) είναι ένας μη κερδοσκοπικός οργανισμός που επικεντρώνεται στη βελτίωση ασφάλειας του λογισμικού. Οι δύο παρακάτω σύνδεσμοι αφορούν κάποιες στατιστικές μελέτες του οργανισμού που πραγματοποιήθηκαν το 2010 και 2013. Να σημειώσουμε ξανά ότι μέσα σε αυτό το διάστημα των τεσσάρων χρόνων η επίθεση injection καταλαμβάνει την πρώτη θέση και στις δύο λίστες.
http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

Τι σημαίνει ακριβώς SQL Injection; Τα τελευταία χρόνια, η τεχνική της επίθεσης SQL Injection χρησιμοποιείται όλο και πιο πολύ από αρκετούς επιτιθέμενους που τους δίνετε η δυνατότητα να "τρέξουν" εντολές της γλώσσας SQL ενάντια σε κάποιον στόχο (πολλές φορές σε κάποιον εξυπηρετητή). Έτσι, κάποιος cracker χρησιμοποιώντας τις ικανότητές του έχει τη δυνατότητα να αποσπάσει σημαντικό πλήθος ευάλωτων πληροφοριών (όπως π.χ. ονόματα χρηστών, κωδικούς πρόσβασης, emails, αριθμοί πιστωτικών καρτών κ.α.) μέσα από τη ΒΔ στην οποία έχει εκτελέσει την επίθεσή του.

Μια τυπική επίθεση SQL Injection

Ας φανταστούμε ότι ήρθαμε σε επαφή με τους διαχειριστές μιας ιστοσελίδας, οι οποίοι μας έχουν αναθέσει να ελέγξουμε τις αντοχές της. Αρχικά, όταν ξεκινήσουμε οφείλουμε να επισκεφθούμε τον ιστότοπο ως απλοί επισκέπτες και εν συνεχεία με κάποιον τρόπο να αποκτήσουμε πρόσβαση με δικαιώματα διαχειριστή (administrator). Με αυτήν την απλή διαδικασία διαπιστώνουμε αν η συγκεκριμένη ιστοσελίδα είναι ασφαλής ή όχι. **Να επισημάνουμε πως όποιες γνώσεις αποκτήσουμε μέσα από κάποιες διαδικασίες δεν πρέπει να τις χρησιμοποιήσουμε ώστε να προβούμε σε κακόβουλες ενέργειες οποιασδήποτε ιστοσελίδας του διαδικτύου** καθώς και επίσης **ίσως χρειαστεί να χρησιμοποιήσουμε δοκιμαστικά κάποιο site για διάφορα tests και παραδείγματα, το οποίο είναι ειδικά διαμορφωμένο για τέτοιου είδους επιθέσεις ώστε να μην υπάρξει κάποιο πρόβλημα με διαχειριστές – ιδιοκτήτες.**

Κατά τη διάρκεια μιας τυπικής επίθεσης SQL Injection η οποία λογικά βασίζεται σε σφάλματα, συνήθως πραγματοποιούμε δοκιμές με κάποιες standard εντολές της SQL[7] στον εξυπηρετητή (server) που έχουμε ως στόχο. Σε περίπτωση που ο server μετά τις δοκιμές μας εμφανίσει λάθη (δηλαδή ανταποκρίνεται θετικά) υπάρχουν πολλές πιθανότητες να είναι ευάλωτος σε SQL Injection. Παρακάτω θα δείξουμε στην πράξη κάποια απλά παραδείγματα τα οποία για λόγους ευχρηστίας θα δίνονται σε μορφή PHP[8].

Παράδειγμα 1ο. Θεωρούμε μία περίπτωση προβολής στοιχείων κάποιου υπαλλήλου από έναν πίνακα με τίτλο "employees" μέσα σε μία ΒΔ της MySQL. Τώρα θα δούμε έναν ευπαθή block κώδικα της PHP ο οποίος εκτελεί μια ερώτηση SELECT στη ΒΔ των στοιχείων του υπαλλήλου.

```
<?php
$qry = "SELECT employeeid, fullname, salary FROM employees " .
     "WHERE employeeid =" . $_GET['employeeid'];
$result = mysql_query($qry);
?>
```

[7] Διάφορες συνηθισμένες εντολές σύνταξης σε γλώσσα SQL που αφορούν επιθέσεις injection, βρίσκονται στον παρακάτω σύνδεσμο: http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet.

[8] PHP είναι μια γλώσσα που σχεδιάστηκε για να βοηθάει στην ανάπτυξη των ιστών καθώς ασχολείται και με γενικής χρήσης προγραμματισμό. Ο κώδικας της έχει τη δυνατότητα να ενσωματώνεται και σε HTML. Περισσότερες πληροφορίες εδώ: https://en.wikipedia.org/wiki/PHP

Σύμφωνα με το παραπάνω, ο προγραμματιστής στοχεύει να εκτελέσει επερωτήσεις που έχουνε μορφή…

```
SELECT employeeid, fullname, salary FROM employees WHERE employeeid = 3
SELECT employeeid, fullname, salary FROM employees WHERE employeeid = 352
SELECT employeeid, fullname, salary FROM employees WHERE employeeid = 590
```

…όπου βλέπουμε το employeeid (θεωρείται πρωτεύον κλειδί στον πίνακα employees) και είναι η τιμή που εισάγεται στην πράξη από τον χρήστη της εφαρμογής (μέσω κάποιου browser χρησιμοποιώντας τη μέθοδο GET του HTTP) π.χ. μπορεί να δίνεται με έναν σύνδεσμο της μορφής: http://www.example.com/employees.php?employeeid=3.

Το πρόβλημα υπάρχει στην τιμή της παραμέτρου GET "employeeid" που δίνεται στον παραπάνω σύνδεσμο, στον οποίο δεν επαληθεύεται με επάρκεια πριν την εκτέλεση της επερώτησης από τον κώδικα. Αυτό σημαίνει πως ένα κακόβουλος χρήστης μπορεί να γράψει την συγκεκριμένη URL προσθέτοντας στο τέλος "OR 1=1", το οποίο θα έχει ως αποτέλεσμα να εκτελεστεί στη ΒΔ η παρακάτω επερώτηση:

```
SELECT employeeid, fullname, salary FROM employees WHERE employeeid=3 OR 1=1
```

…όμως με αυτήν την επερώτηση ο κλάδος WHERE θα ισχύει για κάθε εγγραφή του πίνακα employees, άρα όλες οι εγγραφές επιστρέφονται στη μεταβλητή $result.

Επομένως, ανάλογα με το πως χρησιμοποιείται η μεταβλητή $result ώστε να παρουσιάσει τα δεδομένα στους χρήστες της εφαρμογής στο δίκτυο, τότε ενδέχεται ο εισβολέας να διαπιστώσει πληροφορίες το οποίο δεν πρέπει να γίνει.

Παράδειγμα 2ο. Τώρα ας εξετάσουμε ένα άλλο (ας το πούμε ευάλωτο) block κώδικα PHP για το login σε μια εφαρμογή και τις τιμές (usernames & passwords) που χρησιμοποιούν οι χρήστες σε μία πλατφόρμα για να εισέλθουν σε κάποιο σύστημα.

```
<?php
$username = $_POST['username'];
$password = $_POST['password'];
$qry = "SELECT userid FROM users" .
      " WHERE username='$username' AND password='$password'";
$result = mysql_query($qry);
if (mysql_numrows($result) > 0)
{
   //log in user...
}
?>
```

Οι τιμές των usernames και passwords εισάγονται με τη χρήση μιας web login φόρμας με την τυπική μέθοδο HTTP POST. Όμως, εάν ο εισβολέας στο πεδίο του κωδικού εισάγει την τιμή «bar' OR 1=1 OR username='» τότε από τον προηγούμενο κώδικα PHP προκύπτει η εκτέλεση της επερώτησης…

```
SELECT userid FROM users WHERE
username='foo' AND password='bar' OR 1=1 username='';
```

…η οποία ισχύει πάντα για κάθε εγγραφή στον πίνακα εφόσον 1=1, οπότε το $result θα έχει πάντοτε εγγραφές, ανεξαρτήτως με το τι έχει ήδη εισαχθεί στα πεδία των username και

password. Εν συνεχεία, καθώς η μεταβλητή $result ελέγχεται εάν περιέχει εγγραφές (που με τον παραπάνω τρόπο, αυτήν τη φορά θα έχει) τότε κάνει login τον χρήστη.

Με αυτόν τον τρόπο υπάρχει ενδεχόμενο πρόσβασης στην εφαρμογή (login) από μη εξουσιοδοτημένο πρόσωπο το οποίο δεν κατέχει τα συγκεκριμένα δικαιώματα για κάτι ανάλογο.

Εν τέλει, σε αυτό το παράδειγμα αλλά και στο προηγούμενο (1^{ο}), παρατηρήσαμε το πως μπορεί ένας κακόβουλος χρήστης να παραποιήσει ένα ερώτημα με τη χρήση της SQL με έναν τρόπο που ένας προγραμματιστής ίσως δεν έχει προβλέψει. Σίγουρα τα συγκεκριμένα επερωτήματα θα μπορούσανε να διατυπωθούν με διάφορους άλλους τρόπους σε βάση αυτών που προαναφέραμε (π.χ. μία τυπική περίπτωση είναι η προσπάθεια χρήσης UNION[9] της SQL).

Παράδειγμα 3^{ο}. Σε αυτό το παράδειγμα θα δούμε πολλαπλές εντολές σε SQL εκτελεσμένες μέσα σε ένα επερώτημα στο σύστημα. Ανάμεσα στις εντολές υπάρχει ο γνωστός χαρακτήρας « ; », το ελληνικό ερωτηματικό, το οποίο λειτουργεί διαχωρίζοντας τις εντολές μία προς μία. Εκτελώντας πολλαπλές εντολές μέσα σε ένα επερώτημα, είναι αρκετά σύνηθες στο χώρο των ΒΔ, όμως στην περίπτωση των SQL Injections διατρέχει πολύ μεγάλο κίνδυνο.

Με βάση το πρώτο παράδειγμα θα πράξουμε θεωρώντας ότι το παρακάτω σύστημα ΒΔ είναι της PostgreSQL[10]…

```
<?php
$qry = "SELECT employeeid, fullname, salary FROM employees " .
      "WHERE employeeid =" . $_GET['employeeid'];
$result = pg_query($qry);
?>
```

...εδώ ο προγραμματιστής αναμένει να εισάγει τα δεδομένα εισόδου από συνδέσμους της μορφής: http://www.example.com/employees.php?employeeid=3 και αυτό δίνει αποτέλεσμα εκτέλεσης της εξής επερώτησης:

```
SELECT employeeid, fullname, salary FROM employees
WHERE employeeid = 3
```

Όμως, αυτήν τη φορά ο εισβολέας δίνει μία παραποιημένη διεύθυνση URL χειρονακτικά στον πλοηγητή:

http://www.example.com/employees.php?employeeid=3; DELETE FROM users;

…έτσι θα εκτελεστούν οι παρακάτω δύο εντολές στην pg_query():

```
SELECT employeeid, fullname, salary FROM employees
WHERE employeeid = 3;
```

---

[9] Η SQL UNION είναι ένας τρόπος ένωσης δύο ή περισσότερων αποτελεσμάτων SELECT, τα οποία πρέπει να συντάσσονται κυρίως με ίδιο αριθμό στηλών και ίδιους τύπους δεδομένων. Για περισσότερες πληροφορίες πλοηγηθείτε εδώ: http://www.w3schools.com/sql/sql_union.asp.

[10] Η PostgreSQL είναι μία σχεσιακή ΒΔ ανοικτού κώδικα με αρκετές δυνατότητες και καλή αρχιτεκτονική. Αναλυτικότερα, ανοίξτε τον επόμενο σύνδεσμο: https://el.wikipedia.org/wiki/PostgreSQL. Για την επίσημη ιστοσελίδα, πλοηγηθείτε εδώ: http://www.postgresql.org/.

DELETE FROM users;

…όπου αυτό θα διαγράψει όλα τα δεδομένα του πίνακα users από τη ΒΔ. (Στο παραπάνω παράδειγμα, αντί για την εντολή της διαγραφής θα μπορούσαμε να εκτελέσουμε κάποια διαφορετική εντολή).

Εν τέλει, προσπαθήσαμε να εξηγήσουμε συνοπτικά τις παραπάνω αναφορές για τις ευπάθειες SQL Injections ώστε να περιγραφεί το πρόβλημα με τον καλύτερο δυνατό τρόπο (μέσω μερικών απλών παραδειγμάτων) χρησιμοποιώντας μεθόδους αλλαγής μιας επερώτησης SQL καθώς και για το πώς είναι δυνατόν να εκτελεστούν ολοκληρωμένες εντολές.

1.17) Cross Site Scripting (XSS)

Το Cross Site Scripting είναι ένα από τα πιο διαδεδομένα κενά ασφαλείας διαδικτυακής εφαρμογής, το οποίο συμβαίνει όταν μια εφαρμογή αποκτάει κάποια αναξιόπιστα δεδομένα και τα προωθεί σε έναν web browser δίχως την κατάλληλη έγκριση. Αυτό αφήνει στους επιτιθέμενους το περιθώριο να εκτελέσουν scripts σε browsers των θυμάτων όταν οι ίδιοι επισκέπτονται μια ιστοσελίδα, το οποίο μπορεί να έχει ως αποτέλεσμα να προβαίνουν σε εκβιαστικές ενέργειες στα πόστα των χρηστών, καταστρέφοντας τις ιστοσελίδες και οδηγώντας τον χρήστη σε κακόβουλες ιστοσελίδες.

Επομένως, το XSS βασίζεται στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με τη χρήση HTML κώδικα ή JavaScript μέσα σε κάποιον ιστότοπο.

Ας φανταστούμε πως ένας κακόβουλος χρήστης θα είχε τη δυνατότητα να εισάγει κώδικα σε έναν ιστότοπο, για παράδειγμα μέσω ενός εισόδου κειμένου, ο οποίος κώδικας αφού δε θα φιλτραριζόταν σωστά, θα μπορούσε να προκαλέσει φθορές στον διαχειριστή ή στον επισκέπτη της συγκεκριμένης ιστοσελίδας. Ας πούμε πως μορφοποιεί τον παρακάτω σύνδεσμο:

http://www.example.com/index.html?name=<script>alert(“xss_revealed”)</script>

…έτσι, ο κακόβουλος χρήστης θα μπορούσε να επιτύχει:

- την κλοπή κωδικών/λογαριασμών και διάφορων προσωπικών δεδομένων
- αλλαγή ρυθμίσεων της ιστοσελίδας
- κλοπή των cookies
- ψεύτικη-εσκεμμένη διαφήμιση (π.χ. μέσω ενός συνδέσμου)

Συνεπώς, η ευπάθεια γίνεται αντιληπτή όταν το σύστημα αρχίζει να εμφανίζει σημάδια αδυναμίας και δεν μπορεί να υποστηρίξει τις υποχρεώσεις του, καθώς και να φιλτράρει όλες τις εισόδους έτσι ούτως ώστε να διαχωρίσει τις επιβλαβείς και να τι απορρίψει.

Περισσότεροι από τους ειδικούς διαχωρίζουν τις ευπάθειες από τις XSS επιθέσεις σε δύο βασικές κατηγορίες, τις *μόνιμες* και τις *μη μόνιμες*. Επίσης, δύο άλλες κατηγορίες που μπορούν να χωριστούν είναι οι παραδοσιακές επιθέσεις (οι οποίες προκαλούνται από την πλευρά του εξυπηρετητή) και οι επιθέσεις βασισμένες σε DOM (οι οποίες προκαλούνται από την πλευρά του πελάτη).

Μόνιμες: οι ευπάθειες σε μόνιμες XSS επιθέσεις είναι πολύ καταστροφικές. Οι μόνιμες, προκύπτουν όταν τα δεδομένα τα οποία στέλνονται από κάποιον κακόβουλο χρήστη

αποθηκεύονται στον εξυπηρετητή, ώστε μετά να εμφανίζονται μέσα στις ιστοσελίδες του εξυπηρετητή όταν οι χρήστες κάνουν την πλοήγησή τους μέσα σε αυτές. Ένα γνωστό παράδειγμα τέτοιων επιθέσεων είναι σε online message boards, που εκεί επιτρέπονται οι χρήστες να δημοσιεύσουν μηνύματα σε HTML για να τα δουν άλλοι χρήστες.

Μη μόνιμες: οι ευπάθειες σε μη μόνιμες XSS επιθέσεις είναι οι πιο δημοφιλέστερες. Οι αδυναμίες αυτές προκύπτουν όταν τα δεδομένα που δίνονται από έναν web-client χρησιμοποιούνται επιτόπου από κάποιο script, το οποίο λειτουργεί από την πλευρά του εξυπηρετητή ώστε να εμφανιστεί ένα αποτέλεσμα στον πελάτη, δίχως να έχει προηγηθεί πρώτα έλεγχος και καθαρισμός του αιτήματος που έστειλε ο πελάτης.

Παραδοσιακές & βασισμένες σε DOM ευπάθειες: αυτές οι ευπάθειες δημιουργήθηκαν από την ανάπτυξη των web 2.0 εφαρμογών (δεύτερης γενιάς εφαρμογές). Ενώ στις παραδοσιακές επιθέσεις είναι συνηθισμένο οι ευπάθειες να οφείλονται στον εξυπηρετητή όταν ετοιμάζει μια HTML απάντηση για κάποιον πελάτη, οι επιθέσεις σε DOM κατά το στάδιο της επεξεργασίας των περιεχομένων που εκτελούνται στον πελάτη. Το όνομα αυτών των επιθέσεων προέρχεται από τον τρόπο που απεικονίζονται τα HTML ή XML αντικείμενα, ο οποίος τρόπος και αποκαλείται Document Object Model (DOM).

Ένα παράδειγμα Cross Site Scripting σε λογισμικό Apache Server[11], υπήρχε ένα κενό ασφαλείας στον Tomcat, στον κώδικα ενός αρχείου JavaScript, εν ονόματι sessionsList.jsp. Ο συγκεκριμένος κώδικας χρησιμοποιούσε τις μη ασφαλείς μεταβλητές orderBy και sort. Κάποιος κακόβουλος χρήστης, θα είχε την ικανότητα μέσω ενός text input field να δώσει ως είσοδο JavaScript κώδικα που θα έβλαπτε τον χρήστη που θα επισκεπτόταν το site κάποια στιγμή αργότερα. Ο κώδικας θα μπορούσε να οδηγήσει τον εξυπηρετητή του θύματος σε κάποιον σύνδεσμο (URL) σε επιλογή του κακόβουλου χρήστη, ο οποίος εισβολέας θα είχε την ικανότητα να οργανώσει ξανά καλύτερα την επίθεσή του μέσω JavaScript κώδικα, που αυτήν τη φορά θα έχει αποκτήσει «άδεια» του Apache Server.

Ο κώδικας που αφορούσε την παραπάνω ευπάθεια ήταν την μορφής:

GET/manager/html/sessions?path=/&sort=”><script?alert(‘xss’)</script>order=ASC &action=injectSessions&refresh=Refresh+Sessions+list

Οι εκδόσεις του Apache Tomcat που έχουν το παραπάνω κενό ασφαλείας είναι από την 6.0.2. έως την 6.0.20 εκτός την 6.0.10 και 6.0.11.

Κάτι που πρέπει να γνωρίζουμε, είναι το πώς να εντοπίζουμε εάν μία ιστοσελίδα είναι ευάλωτη σε XSS επιθέσεις και ευπάθειες υπολογιστικών συστημάτων, όπου ο εισβολέας θα μπορούσε να εισάγει τον κακόβουλο κώδικά του προκαλώντας προβλήματα στον διαχειριστή ή τον επισκέπτη του ιστοτόπου. Τα σημεία που παραβιάζονται ως προς τα cross-site-scripts, μπορεί να είναι δύσκολο να αναγνωριστούν και να αφαιρεθούν από μια web app και γι’ αυτό η καλύτερη πρακτική ώστε να αναζητήσει κάποιος αυτά τα τρωτά σημεία, είναι να πραγματοποιήσει μια εκτενή ανασκόπηση του κώδικα αναζητώντας αυτά τα σημεία όπου εισάγει δεδομένα, μέσω μιας φόρμας εισόδου, τα οποία πιθανόν να οδηγούν σε κάποιον HTML output. Μία ποικιλία από HTML tags (π.χ. <img src…>, <iframe…>, <bgsound src…> κ.α.) μπορούν να χρησιμοποιηθούν στο διαδίκτυο, όπως τα Burp Suite, Webnspect, Acunetix, Netsparker, Websecurity, NStalker κ.α., τα οποία μπορούν να χρησιμοποιηθούν ώστε να βρεθούν αυτά τα κακόβουλα λογισμικά, όμως μαζί με τον χειροκίνητο έλεγχο,

[11] Ο Apache HTTP είναι ένας εξυπηρετητής του παγκόσμιου ιστού. Ένας χρήστης που επισκέπτεται έναν ιστότοπο, ο browser που χρησιμοποιεί επικοινωνεί με έναν διακομιστή (server) μέσω του HTTP πρωτοκόλλου, ο οποίος παράγει τις ιστοσελίδες και τις αποστέλλει στο πρόγραμμα πλοήγησης. Περισσότερα στον παρακάτω σύνδεσμο: https://en.wikipedia.org/wiki/Apache_HTTP_Server

καθώς τα πιο πολλά από αυτά τα εργαλεία χρησιμοποιούν συγκεκριμένα πρότυπα αναζήτησης, αγνοώντας τους διαφορετικούς τρόπους κωδικοποίησης ή τις τεχνικές παράβλεψης που μπορεί να χρησιμοποιηθούν.

Γνωρίζουμε πως οι XSS επιθέσεις είναι από τις πιο διαδεδομένες στο διαδίκτυο και γι' αυτό οφείλουμε να ξέρουμε τρόπους αντιμετώπισης αυτού του είδους απειλών. Οι XSS εκμεταλλεύονται διάφορες ευπάθειες των συστημάτων ώστε να πραγματοποιήσουν τις επιθέσεις τους, οι οποίες διαδραματίζονται από κάποιον κακόβουλο χρήστη που στοχεύει να υποκλέψει στοιχεία ταυτότητας χρηστών ώστε να προβεί στις ευαίσθητες πληροφορίες τους και να κατασκοπεύσει την πλοήγησή τους μέσω κάποιας ψεύτικης διαφήμισης. Για να αποφύγουμε το παραπάνω γεγονός, θα πρέπει να εφαρμόσουμε ορισμένους τρόπους προστασίας. Αρχικώς, θα ήταν ωφέλιμο να περνάγαμε όλα τα εξωτερικά δεδομένα μέσα από ένα φίλτρο το οποίο θα αφαιρεί επικίνδυνες λέξεις-κλειδιά καθώς και να επιλέγουμε συνδέσεις δικτύων μόνο από κάποιον κεντρικό δικτυακό τόπο που επιθυμούμε. Πρέπει να είμαστε αρκετά προσεκτικοί όταν διαβάζουμε ένα μήνυμα σε έναν δημόσιο πίνακα από κάποιο πρόσωπο το οποίο δε γνωρίζουμε. Επίσης, μπορούμε να απενεργοποιήσουμε το javascript στις ρυθμίσεις του πλοηγητή μας. Αποφεύγοντας ιστοσελίδες οι οποίες είναι αρκετά "περίεργες" μειώνουμε τις πιθανότητες στο να εκτεθούμε απέναντι σε κάποιον κακόβουλο χρήστη, όμως εάν πρέπει εισέλθουμε σε κάποια ιστοσελίδα, καλό θα ήταν να πραγματοποιήσουμε την πλοήγησή μας από κάποιο virtual box ή από κάποιο guest account που έχουμε δημιουργήσει. Επιπροσθέτως, πρέπει να αποφεύγουμε να αποθηκεύουμε τους κωδικούς μας στον browser που χρησιμοποιούμε γιατί υπάρχουν πολλές πιθανότητες να υποκλαπούν εύκολα. Έτσι, χρησιμοποιώντας κάποιες από τις παραπάνω τακτικές για την αντιμετώπιση των XSS επιθέσεων, είναι σίγουρο πως θα μειώσουμε τις πιθανότητες κακόβουλης παρέμβασης από τους εισβολείς στο δικτυακό μας σύστημα.

Οι XSS επιθέσεις μπορούν να πραγματοποιηθούν δίχως να χρησιμοποιηθούν μέθοδοι με scripts. Υπάρχουν και άλλες ετικέτες που έχουν τις ίδιες ικανότητες, όπως για παράδειγμα: <body onload=alert('test1')> καθώς και άλλα χαρακτηριστικά όπως το onmouseover με τρόπο σύνταξης…

```
<b onmouseover=alert('Wufff!')>click me!</b>
```

…και το onerror με τρόπο σύνταξης…

```
<img src="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>.
```

Παρακάτω θα αναφερθούμε σε μερικά παραδείγματα Cross-Site Scripting επιθέσεων που ενδέχεται οι κακόβουλοι χρήστες να μπορούν να κοινοποιήσουν υλικό σε κάποια αξιόπιστη ιστοσελίδα για την εκμετάλλευση πληροφοριών από χρήστες.

Παράδειγμα 1ο. Έχουμε έναν JSP (Java Server Page) κώδικα ο οποίος διαβάζει στοιχεία, το id και το eid ενός εργαζομένου, από μία αίτηση HTTP η οποία εμφανίζεται στον χρήστη:

```
<% string eid = request.getParameter("eid"); %>
…
Employee ID: <%= eid %>
```

…σε αυτήν τη μορφή. Ο κώδικας σε αυτό το παράδειγμα λειτουργεί σωστά εάν το eid περιέχει μόνο κείμενο με αλφαριθμητικά δεδομένα. Αν το eid έχει μια τιμή που περιλαμβάνει

μετά-χαρακτήρες ή πηγαίο κώδικα, τότε ο κώδικας θα εκτελεστεί από το πρόγραμμα περιήγησης στο δίκτυο καθώς θα αποκρίνεται σε HTTP κώδικα.

Αρχικώς, αυτό δείχνει πως δεν ανήκει σε μεγάλο μέρος μιας ευπάθειας. Όμως, μετά από όλα αυτά, γιατί κάποιος να εισάγει μια URL διεύθυνση η οποία θα προκαλέσει την εκτέλεση ενός επιβλαβή κώδικα στον υπολογιστή; Ο πραγματικός κίνδυνος του παραπάνω ερωτήματος είναι πως ο κακόβουλος χρήστης θα δημιουργήσει την URL που επιθυμεί ώστε να καλύψει τις ανάγκες του και ύστερα, θα χρησιμοποιήσει διάφορα μέσα επικοινωνίας (π.χ. το ηλεκτρονικό ταχυδρομείο) ώστε να δελεάσει το θύμα του, το οποίο θα πλοηγηθεί στη διεύθυνση που ο εισβολέας θα του έχει αποστείλει. Σε περίπτωση που κάποιο από τα θύματα εισέλθει σε κάποιο από αυτά τα links, τότε έχει ήδη ενεργοποιηθεί εν άγνοια του το κακόβουλο περιεχόμενο μέσω της διαδικτυακής εφαρμογής στον δικό του ηλεκτρονικό υπολογιστή. Αυτός ο μηχανισμός της εκμετάλλευσης των ευάλωτων εφαρμογών web είναι γνωστός και ως Reflected XSS (αντανάκλαση cross-site scripting επιθέσεων).

Παράδειγμα 2^{ο}. Το παρακάτω τμήμα JSP κώδικα βάσης δεδομένων είναι σε ερωτήματα, με στοιχεία ενός εργαζόμενου (id, όνομα).

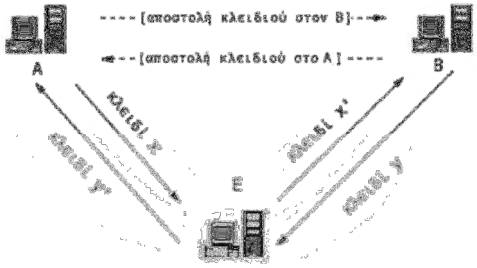
```
<%...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
If (rs != null) {
        rs.next();
        String name = rs.getString("name");
%>

Employee Name: <%= name %>
```

Όπως και στο πρώτο παράδειγμα, ο παραπάνω κώδικας λειτουργεί ορθά όταν οι τιμές και τα ονόματα συμπεριφέρονται σωστά, αλλά αυτό δε σημαίνει ότι θα αποτραπεί κάποια επίθεση. Και πάλι, ο κώδικας μπορεί να γίνει λιγότερο ευάλωτος επειδή η τιμή του ονόματος μπορεί να διαβαστεί από μία ΒΔ, της οποίας τα περιεχόμενα διαχειρίζονται από την εφαρμογή. Ωστόσο, εάν η αξία του ονόματος προέρχεται από στοιχεία του χρήστη τα οποία είναι παρεχόμενα, τότε η ΒΔ μπορεί να γίνει αγωγός για κακόβουλα περιεχόμενα. Δίχως την κατάλληλη επικύρωση σχετικά με όλα τα δεδομένα που είναι αποθηκευμένα στη ΒΔ, κάποιος εισβολέας έχει την ικανότητα να εκτελέσει κακόβουλες εντολές στον web browser του χρήστη. Αυτού του είδους η εκμετάλλευση που ονομάζεται Stored XSS, είναι αρκετά ύπουλη διότι η κακόβουλη ενέργεια πραγματοποιήθηκε στο μέρος που προκλήθηκε, δηλαδή στον αποθηκευτικό χώρο δεδομένων και έτσι είναι αρκετά δύσκολο να εντοπιστεί η απειλή καθώς με αυτόν τον τρόπο αυξάνονται οι πιθανότητες ότι η επίθεση αυτή θα "μολύνει" ολοένα και περισσότερους χρήστες. Αυτή η XSS επίθεση μπορεί να ξεκινήσει την αποστολή της μέσω ενός guestbook για τους επισκέπτες κάποιας ιστοσελίδας. Οι επιτιθέμενοι περιλαμβάνουν εγγραφές στο συγκεκριμένο βιβλίο που αφορά τους επισκέπτες σε μορφή JavaScript και έτσι θα εκτελείται ο κακόβουλος κώδικας εν άγνοια των επισκεπτών.

1.18) Man in the Middle

Η επίθεση man in the middle είναι μια παραβίαση ασφάλειας που ο κακόβουλος χρήστης παρεμβάλλεται ανάμεσα σε δύο χρήστες οι οποίοι γνωρίζονται μεταξύ τους και παρεμποδίζει τη νόμιμη επικοινωνία τους. Εν συνεχεία, ο συγκεκριμένος host ελέγχει τη ροή της επικοινωνίας έχοντας την ικανότητα να αποσπάσει διάφορα στοιχεία και σημαντικές πληροφορίες που στέλνονται αμφίδρομα από τους συμμετέχοντες.

Αυτού του τύπου οι επιθέσεις εφαρμόζονται συνήθως στα Diffie-Hellman[12] πρωτόκολλα, όταν η συμφωνία για την ανταλλαγή κλειδιών πραγματοποιείται δίχως να απαιτείται επικύρωση ταυτότητας (authentication). Στο διπλανό σχήμα απεικονίζεται ένα κύκλωμα με δύο νόμιμους χρήστες (A & B) και έναν κακόβουλο (E) που επιτίθεται, αποστέλλοντας τα χ και ψ κλειδιά με παραλλαγμένες πληροφορίες ώστε να προκαλέσει τον κίνδυνο και τελικώς να επιτύχει τον σκοπό του.



Οι Man in the Middle επιθέσεις χωρίζονται σε δύο μορφές, ο κακόβουλος χρήστης, είτε κρυφακούει τη συνομιλία των νόμιμων χρηστών, είτε αλλοιώνει ανάλογα το μήνυμα εξυπηρετώντας τους απώτερους σκοπούς του. Με τον πρώτο τρόπο της λαθρακρόασης, ο επιτιθέμενος ακούει ένα σύνολο μεταδόσεων από διαφορετικούς hosts ακόμα και αν ο υπολογιστής του επιτιθέμενου δεν συμβάλλει στη συνδιάλεξη αυτή. Πολλοί σχετίζουν αυτόν τον τύπο της επίθεσης με διαρροή, στην οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε κάποιον τρίτο, εν άγνοια των νόμιμων χρηστών. Με τον δεύτερο τρόπο της αλλοίωσης του μηνύματος, ο επιτιθέμενος βασίζεται στην ικανότητα του πρώτο τρόπου που αναφέραμε ακριβώς πιο πάνω. Έτσι, ο επιτιθέμενος παίρνει αυτήν τη μη εξουσιοδοτημένη απόκριση μαζί με ένα ρεύμα δεδομένων (data stream), αλλάζοντας τα περιεχόμενα έτσι ώστε να ικανοποιήσει τον σκοπό του. Πολύ πιθανόν να χρησιμοποιήσει ψευδά στοιχεία, όπως για παράδειγμα αλλάζοντας την IP και MAC διεύθυνσή του, ώστε να μιμηθεί κάποιον άλλον host.

Ακολουθεί ένα απλό παράδειγμα επίθεσης, την οποία θα αναπαραστήσουμε με απλό σχεδιάγραμμα.

Στο παραπάνω σχήμα βλέπουμε τους δύο νόμιμους χρήστες σε κύκλους και τον παράνομο χρήστη σε ορθογώνιο. Η Καλλιόπη από τη μία προσπαθεί να επικοινωνήσει με την Ισμήνη, η οποία βρίσκεται απέναντι. Εν άγνοια των δύο αυτών χρηστών βρίσκεται ο

[12] Το Diffie-Hellman πρωτόκολλο είναι το πρώτο που προτάθηκε ώστε να επιτρέπει σε δύο οντότητες δίχως κάποιο ιστορικό επικοινωνίας, να ανταλλάξουν ένα κοινό κλειδί μέσω ενός επικίνδυνου διαύλου επικοινωνίας ώστε να μην υποκλαπούν οι πληροφορίες τους. Περισσότερες πληροφορίες στον παρακάτω σύνδεσμο: https://el.wikipedia.org/wiki/%CE%A0%CF%81%CF%89%CF%84%CF%8C%CE%BA%CE%BF%CE%BB%CE%BB%CE%BF_Diffie-Hellman

Μενέλαος, ο οποίος προσπαθεί να παρακολουθήσει τη συζήτηση και να αποκομίσει διάφορα στοιχεία δίχως οι δύο γυναίκες να γνωρίζουν την ύπαρξή του.

Βήμα 1^{ο} Καθώς ξεκινάει η επικοινωνία των δύο γυναικών, η πρώτη ζητά κάποιο δημόσιο κλειδί επικοινωνίας στην δεύτερη και αν η δεύτερη στείλει το δεδομένο του δημόσιου κλειδιού τότε ο Μενέλαος θα μπορέσει να το υποκλέψει, το οποίο ουσιαστικά σημαίνει ότι η επίθεση "Man in the Middle" έχει ήδη ξεκινήσει.

Βήμα 2^{ο} Προτού το μήνυμα της δεύτερης φτάσει στην πρώτη, ο κακόβουλος χρήστης το παραποιεί (εάν τον εξυπηρετεί), στέλνοντας έτσι ένα μήνυμα στον προορισμό του, το οποίο συμφέρει τους στόχους του υποκλοπέα.

Βήμα 3^{ο} Η Καλλιόπη λαμβάνει το κλειδί από την Ισμήνη, το οποίο θεωρείται γνήσιο για την πρώτη πιστεύοντας πως ανήκει στην δεύτερη, όμως ο κρυφός μεσολαβητής έχει ήδη κάνει το πρώτο του πρακτικό βήμα με επιτυχία δίχως να εντοπιστεί. Έτσι, η πρώτη βρίσκεται στο στάδιο της κρυπτογράφησης, κρυπτογραφώντας το πλαστό κλειδί του Μενέλαου και προωθώντας το στην Ισμήνη.

Βήμα 4ο Ο Μενέλαος υποκλέπτει το μήνυμα ξανά και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί, αν επιθυμεί το παραποιεί και στη συνέχεια το αποστέλλει κρυπτογραφημένο με το δημόσιο κλειδί της Ισμήνης στην ίδια.

Όταν η τελευταία λαμβάνει το πλαστογραφημένο μήνυμα από τον κακόβουλο χρήστη, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό της κλειδί, θεωρώντας πως το μήνυμα έχει σταλθεί από την Καλλιόπη, δίχως να γνωρίζει πως τα δεδομένα της επικοινωνίας τους έχουν διαρρεύσει, όμως όταν το αντιληφθεί (αν γίνει αντιληπτό) θα είναι πλέον αργά.

2) Λογισμικά που χρησιμοποιήθηκαν

Για την πραγματοποίηση της ψηφιακής ανάλυσής μας χρησιμοποιήσαμε το λειτουργικό σύστημα Kali Linux που έχει βάση την έκδοση Debian και τα προγράμματα OpenVas, OWASP ZAP για ανάλυση και διαχωρισμό των διαφόρων αποτελεσμάτων που εμφάνισαν.

Kali Linux (penetration testing distribution)

Το λειτουργικο σύστημα που χρησιμοποιήσαμε σαν βάση για την εκτέλεση διαφόρων ειδών αναλύσεις προς το πληροφοριακό σύστημα βρίσκονται προεγκατεστημένα στο παρόν λειτουργικό. Το εν λόγω λειτουργικό είναι δημιουργία της ομάδας Offensive Security και έχει προεγκατεστημένα εξειδικευμένα εργαλεία για την ανάλυση και την εισχώρηση σε πληροφοριακά συτήματα και κάθε τι ψηφιακό. Είναι ελεύθερο λογισμικό (open source) και βρίσκεται στην επίσημη σελίδα των Kali Linux. Δίνει την δυνατότητα στο χρήστη την επιλογή με τι θέλει να δουλέψει όπως γραφικό περιβάλλον (gui), γραμμή εντολών (terminal) πάνω στην έκδοση για λογισμικά Unix Gnome 3 (γραφικό περιβάλλον χρήστη). <<https://www.kali.org/>>

Λογισμικά Ανάλυσης

Για την ανάλυση του πληροφοριακού συστήματος χρησιμοποιήσαμε αυτοματοποιημένες πλατφόρμες ανάλυσης (frameworks) οι οποίες ειδικεύονται στην ανάλυση ψηφιακών συστημάτων και εμφανίζουν τα αποτελέσματα με συγκεντρωτικό τρόπο ώστε να βοηθήσουν το χρήστη στην ανάλυση-επεξήγηση των αποτελεσμάτων καθώς και την αναζήτηση λεπτομερειών με εύκολο τρόπο. Παρακάτω θα αναφέρουμε λίγα λόγια για όλα τα εργαλεία που χρησιμοποιήθηκαν καθόλη τη διάρκεια της ανάλυσης του πληροφοριακού συστήματος του Ιδρύματος. Αυτά τα εργαλεία είναι το OpenVas και το OWASP ZAP.

2.1) OpenVas (Open Vulrenability Assesment System)

Το OpenVas είναι μία αυτοματοποιημένη και ευκολόχρηστη πλατφόρμα για την ανάλυση συγκεκριμένων ηλεκτρονικών διευθύνσεων καθώς και πλήθος ηλεκτρονικών διευθύνσεων ταυτόχρονα και εμφάνιση των αποτελεσμάτων ομαδοποιημένα. Το συγκεκριμένο εργαλείο έχει τη δική του βάση δεδομένων η οποία ενημερώνεται από τους δημιουργούς της για την κρισιμότητα-σοβαρότητα του κάθε αποτελέσματος. Επίσης παρέχει στα αποτελέσματα , ποσοστά επιτυχίας κάποιας επίθεσης σε τρύπες ασφαλείας που έχει βρει καθώς και προτεινόμενους τρόπους αντιμετώπισης με παραπομπές σε επίσημες ηλεκτρονικές διευθύνσεις που παρέχουν εξειδικευμένη βοήθεια για κάθε τρύπα των συστημάτων. Είναι γραμμένο αρχικά σε γλώσσα NASL (Nessus Attack Scripting Language) και από την έκδοση 2.0 με την OVAL (Open Vulnerability and Assessment Language). Δίνεται η δυνατότητα στο χρήστη να δημιουργήσει δικά του “scripts” και να τα ενσωματώσει στο εργαλείο αυτό με ελάχιστες γνώσεις προγραμματισμού. Ο τρόπος χρησιμοποίησης του εργαλείου αυτού γίνεται μέσω του Internet Browser με τοπικη διεύθυνση που θέτει ο χρήστης κατά τη παραμετροποίηση του προγράμματος. Διατίθεται δωρεάν από την επίσημη ηλεκτρονική διεύθυνση καθώς και ο κώδικας που είναι γραμμένο μιας κ έχει την ιδιότητα του ανοιχτού λογισμικού (open source). <<http://www.openvas.org/>>

2.1.1) Αξιολόγηση της Ανίχνευσης (Quality Of Detection - QOD)

QoD	Κατηγορία(ες) QoD	Λεπτομέρειες
100%	exploit	Η ανίχνευση έγινε μέσω αξιοποίησης της αδυναμίας συστήματος (exploit) και είναι ολοκληρωτικά επιβεβαιωμένο.
99%	remote_vul	Απομακρυσμένοι ενεργοί έλεγχοι (εκτέλεση κώδικα-code execution, επίθεση διέλευσης- traversal attack, έγχυση sql-sql injection, κ.α.) όπου η ανταπόκριση δείχνει καθαρά τη παρουσία της αδυναμίας συστήματος.
98%	remote_app	Απομακρυσμένοι ενεργοί έλεγχοι (εκτέλεση κώδικα-code execution, επίθεση διέλευσης- traversal attack, έγχυση sql-sql injection, κ.α.) όπου η ανταπόκριση δείχνει καθαρά τη παρουσία της αδυναμίας της εφαρμογης.
97%	package	Πιστοποιημένα πακέτα επιβεβαιωμένα για συστήματα Linux.
97%	registry	Πιστοποιημένα αρχεία-registry επιβεβαιωμένα για συστήματα Windows.
95%	remote_active	Απομακρυσμένοι ενεργοί έλεγχοι (εκτέλεση κώδικα-code execution, επίθεση διέλευσης - traversal attack, έγχυση sql - sql injection, κ.α.) όπου η ανταπόκριση δείχνει να υπάρχει παρουσία της αδυναμίας της εφαρμογης ή του συστήματος. Κάτω από σπάνιες περιπτώσεις είναι δυνατόν να είναι λάθος εκτίμηση.
80%	remote_banner	Απομακρυσμένοι ελέγχοι τίτλου-banner εφαρμογών δείχνουν την έκδοση της εφαρμογής. Πολλά προιόντα το έχουν αυτό.
80%	executable_version	Πιστοποιημένες εκτελέσιμες εκδόσεις ελέγχουν για Linux ή Windows συστήματα όπου η εφαρμογή προσφέρει επιπλέον πακέτα στις εκδόσεις.
70%	remote_analysis	Απομακρυσμένος έλεγχος που κάνει ανάλυση αλλά δεν είναι πάντα αξιόπιστος.
50%	remote_probe	Απομακρυσμένος έλεγχος σε ενδιάμεσα συστήματα (firewalls) μπορεί να προσποιηθούν απαντώντας θετικά ώστε να μην είναι ξεκάθαρο ότι απάντησε η εφαρμογή η ίδια.
30%	remote_banner_unreliable	Απομακρυσμένος έλεγχος τίτλου-banner εφαρμογών που δεν προσφέρουν πακέτα στην αναγνώριση της έκδοσης.
30%	executable_version_unreliable	Πιστοποιημένες εκτελέσιμες εκδόσεις ελέγχουν για Linux συστήματα όπου εφαρμογές δεν προσφέρουν πακέτα στη αναγνώριση της έκδοσης.
1%	general_note	Γενικές πληροφορίες για δυνητικές αδυναμίες χωρίς να υπάρχουν παρούσες εφαρμογές.

2.1.2) Header overflow against HTTP proxy (βλ. εικόνα 3.1.1)

Rate -> 7.5 (High)
QOD -> 99%
Port -> 80 / tcp

Περίληψη:
Ήταν δυνατό να εξοντώσει το πληρεξούσιο (proxy) HTTP στέλνοντας ένα άκυρο αίτημα με πολύ μεγάλη επικεφαλίδα (header).
Ένας cracker μπορεί να εκμεταλλευτεί αυτήν την ευπάθεια για να κρασάρει το διακομιστή μεσολάβησης συνεχώς ή ακόμα και να εκτελέσει αυθαίρετο κώδικα στο σύστημα.

Αποτέλεσμα: Ανίχνευση ευπάθειας
Ευπάθεια εντοπίστηκε σύμφωνα με την μέθοδο ανίχνευσης ευπάθειας.

Λύση:
Αναβάθμιση του λογισμικού.

Αναφορές:
CVE: CVE-2002-0133
ΠΡΟΣΦΟΡΑ: 3904, 3905

2.1.3) spank.c (βλ. εικόνα 3.1.2)

Rate -> 5.0 (Medium)
QOD -> 99%
Port-> general / tcp

Περίληψη:
Το μηχάνημα απαντάει σε πακέτα TCP που προέρχονται από μια διεύθυνση πολλαπλής διανομής (multicast). Αυτό είναι γνωστό ως «spank» επίθεση άρνησης υπηρεσίας.

Ένας εισβολέας μπορεί να χρησιμοποιήσει αυτό το ελάττωμα, να κλείσει αυτόν το διακομιστή και τον κορεσμό του δικτύου σας, αποτρέποντας έτσι στο να λειτουργεί σωστά. Αυτό θα μπορούσε επίσης να χρησιμοποιηθεί για να τρέξει stealth σαρώσεις κατά το μηχάνημά σας.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Το μηχάνημά σας κράσαρε όταν έλαβε ένα πακέτο TCP που έρχεται από μια διεύθυνση πολλαπλής διανομής (multicast). Αυτό είναι γνωστό ως «spank» επίθεση άρνησης υπηρεσιών.
Ένας εισβολέας μπορεί να χρησιμοποιήσει αυτό το ελάττωμα, να κλείσει αυτόν το server, έτσι εμποδίζει στο να λειτουργεί σωστά.

Λύση:
Επικοινωνήστε με το πωλητή του λειτουργικού σας συστήματος για μια ενημερωμένη έκδοση. Φιλτράρει διευθύνσεις multicast (224.0.0.0/4)

2.1.4) OpenSSL πολλαπλές ευπάθειες - 02 May16 (Windows) (βλ. εικ. 3.1.3 & 3.1.4)

Rate -> 10.0 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτός ο υπολογιστής τρέχει OpenSSL και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 1.0.1c
Σταθερή έκδοση: 1.0.1o

Επίπτωση:
Η επιτυχής εκμετάλλευση θα επιτρέψει σε έναν απομακρυσμένο εισβολέα να εκτελέσει αυθαίρετο κώδικα ή να προκαλέσει άρνηση υπηρεσίας (υπερχείλιση buffer και διαφθορά μνήμης).

Επίπεδο επιπτώσεων: Σύστημα / Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε OpenSSL 1.0.1o ή 1.0.2c ή αργότερα. Για ενημερώσεις ανατρέξτε στην https://www.openssl.org

Επηρεάζονται Λογισμικά / OS:
Εκδόσεις openSSL 1.0.1 πριν 1.0.1o, και 1.0.2 πριν 1.0.2c στα Windows.

Ευπάθεια insight:
Το ελάττωμα υπάρχει ως αναλυτή ASN.1 (συγκεκριμένα, d2i_ASN1_TYPE) μπορούν να παρερμηνεύσουν μια μεγάλη καθολική ετικέτα ως αρνητική τιμή μηδέν και αν μια εφαρμογή αποσειριοποιήσει μη αξιόπιστη δομή ASN.1 που περιέχει ένα οποιοδήποτε τομέα, και αργότερα τα επανασειριοποιεί, αυτό μπορεί να προκαλέσει μία -εκτός των ορίων- εγγραφή.

Αναφορές:
CVE: CVE-2016-2108
CERT: DFN-CERT-2016-1160, DFN-CERT-2016-1103, DFN-CERT-2016-1092, DFN-CERT-2016-1091, DFN-CERT-2016-1026, DFN-CERT-2016-0867, DFN-CERT-2016-0815, DFN-CERT-2016-0765, DFN-CERT-2016-0702

2.1.5) OpenSSL πολλαπλές ευπάθειες - 01 May16 (Windows) (βλ. εικ. 3.1.7 & 3.1.8)

Rate -> 10.0 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτό ο υπολογιστής τρέχει OpenSSL και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 1.0.1c
Σταθερή έκδοση: 1.0.1s

Επίπτωση:
Η επιτυχής εκμετάλλευση θα επιτρέψει σε έναν απομακρυσμένο εισβολέα να προκαλέσει άρνηση εξυπηρέτησης, για να προκαλέσει διαρροή μνήμης, για να εκτελέσει αυθαίρετο κώδικα και να παρακάμψει τους περιορισμούς ασφαλείας και κάποιες απροσδιόριστες επιπτώσεις.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix)
Αναβάθμιση σε 1.0.1s OpenSSL ή 1.0.2g. Για ενημερώσεις ανατρέξτε στην https://www.openssl.org

Επηρεάζονται λογισμικά / OS:
Εκδόσεις OpenSSL 1.0.1 πριν 1.0.1s και 1.0.2 πριν 1.0.2g στα Windows.

Επίγνωση ευπάθειας:
Πολλαπλά ελαττώματα οφείλονται σε:

- Ένα διπλό χωρίς ευπάθεια κώδικα DSA.
- Ένα θέμα ευπάθειας, διαρροή μνήμης στις αναζητήσεις στη βάση δεδομένων SRP, χρησιμοποιώντας τη λειτουργία «SRP_VBASE_get_by_user».
- Ένα ελάττωμα υπερχείλισης ακεραίου σε ορισμένες λειτουργίες «BIGNUM», που οδηγεί σε dereference NULL δείκτη ή καταστροφή της μνήμης σωρού που βασίζεται.
- Μια ακατάλληλη επεξεργασία των χορδών μορφή στις λειτουργίες «BIO_ * printf».
- Μια επίθεση κανάλι πλευρά για εκθετοποίηση.
- Η λειτουργία «doapr_outch» στο σενάριο «crypto / bio / b_print.c» δεν επαληθεύει την επιτυχία μιας ορισμένης κατανομής μνήμης.

Αναφορές:
CVE: CVE-2016-0705, CVE-2016-0798, CVE-2016-0797, CVE-2016-0799, CVE-2016-0702, CVE-2016-2842
CERT: DFN-CERT-2016-1245, DFN-CERT-2016-1175, DFN-CERT-2016-1174, DFN-CERT-2016-1103, DFN-CERT-2016-1026, DFN-CERT-2016-0951, DFN-CERT-2016-0890, DFN-CERT-2016-0841, DFN-CERT-2016-0815, DFN-CERT-2016-0803, DFN-CERT-2016-0789, DFN-CERT-2016-0765, DFN- CERT-2016-0699, DFN-CERT-2016-0698, DFN-CERT-2016-0644, DFN-CERT-2016-0499, DFN-CERT-2016-0496, DFN-CERT-2016-0465,

DFN-CERT- 2016-0459, DFN-CERT-2016-0453, DFN-CERT-2016-0403, DFN-CERT-2016-0388, DFN-CERT-2016-0360, DFN-CERT-2016-0359, DFN-CERT-2016- 0357

2.1.6) OpenSSL πολλαπλές ευπάθειες - 01 May16 (Windows) (βλ. εικ. 3.1.5 & 3.1.6)

Rate-> 7.8 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτός ο υπολογιστής τρέχει OpenSSL και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 1.0.1c
Σταθερή έκδοση: 1.0.1t

Επίπτωση:
Η επιτυχής εκμετάλλευση θα επιτρέψει σε έναν απομακρυσμένο εισβολέα να πραγματοποιήσει επίθεση "Man In The Middle", να αποκτήσει πρόσβαση σε δυνητικά ευαίσθητες πληροφορίες και να προκαλέσει συνθήκη άρνησης εξυπηρέτησης.

Επίπεδο αντίκτυπου: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε OpenSSL 1.0.1t ή 1.0.2h. Για ενημερώσεις ανατρέξτε στην https://www.openssl.org

Επηρεάζονται λογισμικά / OS:
Εκδόσεις OpenSSL 1.0.1 πριν 1.0.1t και 1.0.2 πριν 1.0.2h στα Windows.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Μια υπερχείλιση ακεραίου στη λειτουργία EVP_EncryptUpdate σε σενάριο «crypto / EVP / script evp_enc.c» στο OpenSSL.
- Μια υπερχείλιση ακεραίου στη λειτουργία EVP_EncodeUpdate σε σενάριο «crypto / EVP / script encode.c» στο OpenSSL.
- Ένα σφάλμα στη λειτουργία «asn1_d2i_read_bio» σε σενάριο «crypto / ASN1 / a_d2i_fp.c» στην εφαρμογή ASN.1 BIO στο OpenSSL.
- Ένα σφάλμα στη λειτουργία του «X509_NAME_oneline» στην «crypto / X509 / x509_obj.c» στο OpenSSL.
- Ένας εισβολέας "Man In The Middle" χρησιμοποιεί μία padding επίθεση μαντείου για να αποκρυπτογραφήσει την κυκλοφορία, όταν η σύνδεση χρησιμοποιεί κρυπτογράφηση AES KTK και την υποστήριξη του διακομιστή AES-NI.

Αναφορές:

CVE: CVE-2016-2176, CVE-2016-2109, CVE-2016-2106, CVE-2016-2107, CVE-2016-2105
CERT: DFN-CERT-2016-1372, DFN-CERT-2016-1175, DFN-CERT-2016-1174, DFN-CERT-2016-1169, DFN-CERT-2016-1166, DFN-CERT-2016-1160, DFN-CERT-2016-1103, DFN-CERT-2016-1092, DFN-CERT-2016-1091, DFN-CERT-2016-1026, DFN-CERT-2016-0951, DFN-CERT-2016-0815, DFN- CERT-2016-0765, DFN-CERT-2016-0740, DFN-CERT-2016-0702

2.1.7) P-smash DoS (ICMP 9 flood) **(βλ. εικονα 3.1.9)**

Rate -> 7.8 (High)
QOD -> 99%
Port -> γενική / tcp

Περίληψη:
Ήταν δυνατό να συντριβεί το απομακρυσμένο μηχάνημα πλημμυρίζοντας με τύπο 9 πακέτα ICMP.
Ένα cracker μπορεί να χρησιμοποιήσει αυτήν την επίθεση για να κρασάρει συνεχώς τον υπολογιστή, εμποδίζοντάς τον από το να λειτουργεί σωστά.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Ευπάθεια εντοπίστηκε σύμφωνα με την ευπάθεια μέθοδο ανίχνευσης.

Λύση:
Αναβαθμίστε το λειτουργικό σύστημα των Windows 9x ή να το αλλάξετε.

Παραπομπή: http://support.microsoft.com/default.aspx?scid=KB en-us q216141

2.1.8) Php πολλαπλές ευπάθειες - 01 April16 (Windows) (βλ. είκονα 3.1.10 & 3.1.11)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 5.4.4
Σταθερή έκδοση: 5.5.33

Επίπτωση:
Επιτυχής αξιοποίηση της ευπάθειας μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να αποκτήσουν πρόσβαση σε δυνητικά ευαίσθητες πληροφορίες και να διεξάγουν μια άρνηση υπηρεσίας (διαφθοράς μνήμης και συντριβή εφαρμογής).
Επίπεδο αντίκτυπου: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php έκδοση 5.5.33 ή 5.6.19 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Php εκδόσεις πριν από 5.5.33, και 5.6.x πριν από 5.6.19 για τα Windows.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Ένα λάθος χρήση-μετά-δωρεάν script wddx.c στην επέκταση WDDX στην PHP.
- Ένα λάθος στη λειτουργία phar_parse_zipfile στο zip.c script στην επέκταση PHAR στην PHP.

Αναφορές:
CVE: CVE-2016-3142, CVE-2016-3141
CERT: DFN-CERT-2016-1004, DFN-CERT-2016-0972, DFN-CERT-2016-0775, DFN-CERT-2016-0676, DFN-CERT-2016-0659

2.1.9) Λειτουργία «phar_fix_filepath» php stack ευπάθειας υπερχείλισης buffer March16 (Windows) (βλ. εικόνα 3.1.12 & 3.1.13)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής στο θέμα ευπάθειας υπερχείλισης buffer.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 5.4.4
Σταθερή έκδοση: 5.4.43

Επίπτωση:
Επιτυχής αξιοποίηση της ευπάθειας μπορεί να επιτρέψει στους απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετο κώδικα στο πλαίσιο της διαδικασίας της PHP. Αποτυχημένες προσπάθειες εκμεταλλεύσης της ευπάθειας πιθανότατα θα συντρίψουν το διακομιστή.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php έκδοση 5.4.43 ή 5.5.27 ή 5.6.11 ή αργότερα. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Php εκδόσεις πριν 4.5.43, 5.5.x πριν από 5.5.27, και 5.6.x πριν από 5.6.11 για τα Windows.

Ευπάθεια insight:
Το ελάττωμα οφείλεται σε ανεπαρκή όριο ελέγχων για τον χρήστη εκεί που παρέχεται είσοδος από τη λειτουργία «phar_fix_filepath» σε σενάριο “ext/phar/phar.c”.

Αναφορές:
CVE: CVE-2015-5590
ΠΡΟΣΦΟΡΑ: 75.970
CERT: CB-K15 / 1439, CB-K15 / 1261, CB-K15 / 1147, DFN-CERT-2016-1004, DFN-CERT-2016-0460, DFN-CERT-2015-1515, DFN-CERT-2015- 1335, DFN-CERT-2015-1203

2.1.10) Php «serialize_function_call» λειτουργία τύπου σύγχυσης ευπάθειας March16 (Windows) (βλ. εικόνα 3.1.14 & 3.1.15)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Ο υπολογιστής αυτός έχει εγκατασταθεί με php και είναι επιρρεπείς σε απομακρυσμένη εκτέλεση κώδικα ευπάθειας.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 5.4.4
Σταθερή έκδοση: 5.4.45

Επίπτωση:
Επιτυχής αξιοποίηση της ευπάθειας μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετο κώδικα στο περιβάλλον του χρήστη που εκτελεί την εφαρμογή που επηρεάζεται. Αποτυχημένες προσπάθειες εκμεταλλεύσης της ευπάθειας θα προκαλέσει πιθανόν μια κατάσταση άρνησης υπηρεσίας.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php έκδοση 5.4.45 ή 5.5.29 ή 6.5.13 ή νεότερη. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Php εκδόσεις πριν 4.5.45, 5.5.x πριν από 5.5.29, και 5.6.x πριν 6.5.13 για τα windows.

Ευπάθεια insight:
Το ελάττωμα οφείλεται στη «SoapClient __call» μέθοδο όπου το “ext/soap/soap.c” script δεν διαχειρίζεται σωστά τις κεφαλίδες.

Αναφορές:
CVE: CVE-2015-6836
ΠΡΟΣΦΟΡΑ: 76.644
CERT: CB-K15 / 1571, CB-K15 / 1561, CB-K15 / 1478, CB-K15 / 1439, CB-K15 / 1415, CB-K15 / 1337, DFN-CERT-2016-1004, DFN-CERT- 2016-0460, DFN-CERT-2015-1658, DFN-CERT-2015-1644, DFN-CERT-2015-1556, DFN-CERT-2015-1515, DFN-CERT-2015-1493, DFN-CERT-2015- 1407

2.1.11) Php πολλαπλές ευπάθειες - 01 March16 (Windows) **(βλ. εικόνα 3.1.16 & 3.1.17)**

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 5.4.4
Σταθερή έκδοση: 5.4.44

Επίπτωση:
Επιτυχής αξιοποίηση της ευπάθειας μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετο κώδικα και να δημιουργήσουν ή να αντικαταστήσουν αυθαίρετα αρχεία στο σύστημα και αυτό μπορεί να οδηγήσει σε δρομολόγηση περαιτέρω επιθέσεων.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php έκδοση 5.4.44 ή 5.5.28 ή 5.6.12 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Php εκδόσεις πριν 4.5.44, 5.5.x πριν από 5.5.28, και 5.6.x πριν από 5.6.12 για τα windows.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Μια πολλαπλή χρήση ελεύθερων τρωτών σημείων στην SPL unserialize εφαρμογή.
- Μια ανεπαρκής επικύρωση του χρήστη που παρέχονται εισροές από «/phar_object.c» Phar σενάριο.

Αναφορές:
CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
ΠΡΟΣΦΟΡΑ: 76737, 76739, 76735
CERT: CB-K15 / 1571, CB-K15 / 1439, CB-K15 / 1415, CB-K15 / 1261, DFN-CERT-2016-1004, DFN-CERT-2016-0460, DFN-CERT-2015-1658, DFN-CERT-2015-1515, DFN-CERT-2015-1493, DFN-CERT-2015-1335

2.1.12) OpenSSL πολλαπλές Denial of Service ευπάθειες - 01 Nov15 (Windows) (βλ. εικόνα 3.1.18 & 3.1.19)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη
Αυτός ο υπολογιστής τρέχει OpenSSL και είναι επιρρεπής σε πολλαπλές άρνησεις των τρωτών σημείων εξυπηρέτησης.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη έκδοση: 1.0.1c
Σταθερή έκδοση: 1.0.1h

Επίπτωση:
Η επιτυχής εκμετάλλευση θα επιτρέψει στους επιτιθέμενους να προκαλέσουν άρνηση υπηρεσίας.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε OpenSSL 0.9.8za ή 1.0.0m ή 1.0.1h ή νεότερη. Για ενημερώσεις ανατρέξτε στην https://www.openssl.org

Επηρεάζονται λογισμικά / OS:
OpenSSL εκδόσεις πριν 0.9.8za, 1.0.0 πριν 1.0.0m, και 1.0.1 πριν 1.0.1h στα windows.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Έναν ακέραιο underflow στη λειτουργία «EVP_DecodeUpdate» στην «crypto / EVP / encode.c» σενάριο για την εφαρμογή base64 - αποκωδικοποίηση.
- Μνήμη ευπάθειας κατά το χειρισμό δομών δεδομένων.

Αναφορές:
CVE: CVE-2015-0292, CVE-2014-8176
ΠΡΟΣΦΟΡΑ: 73228, 75159
CERT: CB-K15 / 1266, CB-K15 / 1059, CB-K15 / 0948, CB-K15 / 0816, CB-K15 / 0802, CB-K15 / 0509, CB-K15 / 0384, CB-K15 / 0365, CB-K15 / 0364, DFN-CERT-2015-1332, DFN-CERT-2015-1113, DFN-CERT-2015 με 0997, DFN-CERT-2015 έως 0859, DFN-CERT-2015-0844, DFN-CERT- 2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374

2.1.13) Php πολλαπλή απομακρυσμένη εκτέλεση κώδικα ευπάθειας July15 (Windows) (βλ. εικόνα 3.1.20 & 3.1.21)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένο Έκδοση: 5.4.4
Σταθερή Έκδοση: 05/04/48

Επίπτωση:
Αξιοποιώντας επιτυχώς αυτό το ζήτημα μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετο κώδικα μέσω κάποιων δημιουργημένων διαστάσεων.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php 5.4.38 ή 5.5.22 ή 5.6.6 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Εκδόσεις php πριν 5.4.38, 5.5.x πριν από 5.5.22, και 5.6.x πριν 5.6.6.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Πολλαπλές χρήσεις ελεύθερων τρωτών σημείων στο σενάριο “ext/date/php_date.c” script.
- Συσσόρευση λόγω της υπερχείλησης του buffer στην λειτουργία “enchant_broker_request_dict” σε “ext/enchant/enchant.c” script.

Αναφορές:
CVE: CVE-2015-0273, CVE-2014-9705
ΠΡΟΣΦΟΡΑ: 73031, 72701
CERT: CB-K15 / 1561, CB-K15 / 1437, CB-K15 / 0966, CB-K15 / 0901, CB-K15 / 0854, CB-K15 / 0806, CB-K15 / 0769, CB-K15 / 0757, CB-K15 / 0665, CB-K15 / 0482, CB-K15 / 0362, CB-K15 / 0358, CB-K15 / 0278, CB-K15 / 0222, DFN-CERT-2016-1004, DFN-CERT-2015- 1644, DFN-CERT-2015-1514, DFN-CERT-2015-1017, DFN-CERT-2015 έως 0956, DFN-CERT-2015 έως 0900, DFN-CERT-2015-0842, DFN-CERT-2015 έως 0809, DFN-CERT-2015-0794, DFN-CERT-2015-0697, DFN-CERT-2015-0505, DFN-CERT-2015-0371, DFN-CERT-2015-0370, DFN-CERT-2015-0286, DFN- CERT-2015-0228

2.1.14) Php πολλαπλές ευπάθειες - 03 June15 (Windows) (βλ. εικόνα 3.1.22 & 3.1.23)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη Έκδοση: 5.4.4
Σταθερή Έκδοση: 5.4.40

Επίπτωση:
Η επιτυχώς αξιοποίηση του ζητήματος μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να προκαλέσουν άρνηση υπηρεσίας, για την απόκτηση ευαίσθητων πληροφοριών από τη μνήμη της διαδικασίας και να εκτελέσουν αυθαίρετο κώδικα μέσω δημιουργημένων διαστάσεων.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php 5.4.40 ή 5.5.24 ή 5.6.8 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Εκδόσεις php πριν 5.4.40, 5.5.x πριν από 5.5.24, και 5.6.x πριν 5.6.8.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Πολλαπλές στοίβες με βάση υπερχειλισμέμου buffer στη λειτουργία «phar_set_inode» σε script “phar_internal.h” σε PHP.
- Θέματα ευπάθειας στο «phar_parse_metadata» και λειτουργίες «phar_parse_pharfile» στο “ext/phar/phar.c” script σε PHP.
- Ένα μηδενικό σημείο ελαττώματος στη λειτουργία «build_tablename» στο “ext/pgsql/pgsql.c” script, που ενεργοποιείται κατά την ένδειξη επιστρεφόμενων μηδενικών τιμών.

Αναφορές:
CVE: CVE-2015-3329, CVE-2015-3307, CVE-2015-2783, CVE-2015-1352
CERT: CB-K15 / 1437, CB-K15 / 1188, CB-K15 / 0966, CB-K15 / 0880, CB-K15 / 0854, CB-K15 / 0806, CB-K15 / 0769, CB-K15 / 0763, CB-K15 / 0757, CB-K15 / 0665, CB-K15 / 0648, CB-K15 / 0561, CB-K15 / 0552, CB-K15 / 0207, DFN-CERT-2016-1004, DFN-CERT-2015- 1514, DFN-CERT-2015-1252, DFN-CERT-2015-1017, DFN-CERT-2015 -0926, DFN-CERT-2015 έως 0900, DFN-CERT-2015-0842, DFN-CERT-2015 έως 0809, DFN-CERT-2015-0803, DFN-CERT-2015-0794, DFN-CERT-2015-0697, DFN-CERT-2015-0677, DFN-CERT-2015-0583, DFN-CERT-2015-0579, DFN- CERT-2015-0212

2.1.15) Php πολλαπλές ευπάθειες - 02 June15 (Windows) (βλ. εικόνα 3.1.24 & 3.1.25)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη Έκδοση: 5.4.4
Σταθερή Έκδοση: 5.4.41

Επίπτωση:
Η επιτυχής αξιοποίηση του ζητήματος μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να προκαλέσουν άρνηση υπηρεσίας. Η παράκαμψη προορίζει περιορισμούς επέκτασης και πρόσβασης, ώστε να μην εκτελέστουν απρόσμενα τα αρχεία ή οι καταλόγοι με τα ονόματα, μέσω δημιουργημένων διαστάσεων και απομακρυσμένων διακομιστών FTP ώστε να εκτελέσουν αυθαίρετο κώδικα.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php 5.4.41 ή 5.5.25 ή 5.6.9 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Εκδόσεις php πριν 5.4.41, 5.5.x πριν από 5.5.25, και 5.6.x πριν 5.6.9.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Μία αλγοριθμική ευπάθεια, που προξενεί πολυπλοκότητα στη λειτουργία «multipart_buffer_headers» στο "main/rfc1867.c" script σε PHP.
- Μία εφαρμογή «pcntl_exec» στην PHP περικόπτει μια διαδρομή μόλις συναντήσει έναν \x00 χαρακτήρα.
- Έναν ακέραιο υπερχείλισης στην «ftp_genlist» λειτουργία, και στην λειτουργία του "ext/ftp/ftp.c" script στην PHP.
- Η λειτουργία του «phar_parse_tarfile» script σε "ext/phar/tar.c" στην PHP, δεν ελέγχει αν ο πρώτος χαρακτήρας του ονόματος αρχείου είναι διαφορετικός από τον \0 χαρακτήρα.

Αναφορές:
CVE: CVE-2015-4026, CVE-2015-4025, CVE-2015-4024, CVE-2015-4022, CVE-2015-4021
CERT: CB-K15 / 1188, CB-K15 / 1082, CB-K15 / 1031, CB-K15 / 0973, CB-K15 / 0966, CB-K15 / 0942, CB-K15 / 0923, CB-K15 / 0880, CB-K15 / 0854, CB-K15 / 0769, CB-K15 / 0763, CB-K15 / 0759, CB-K15 / 0703, DFN-CERT-2016-1004, DFN-CERT-2015-1252, DFN-CERT- 2015-1139, DFN-CERT-2015-1083, DFN-CERT-2015-1021, DFN-CERT-

2015-1017, DFN-CERT-2015-0989, DFN-CERT-2015-0973, DFN-CERT-2015- 0926, DFN-CERT-2015 με 0900, DFN-CERT-2015 - 0809, DFN-CERT-2015 έως 0803, DFN-CERT-2015-0797, DFN-CERT-2015 – 0732

2.1.16) Php πολλαπλές ευπάθειες - 01 June15 (Windows) (βλ. εικόνα 3.1.26 & 3.1.27)

Rate -> 7.5 (High)
QOD -> 80%
Port -> 8080 / tcp

Περίληψη:
Αυτή η υποδοχή έχει εγκατασταθεί με php και είναι επιρρεπής σε πολλαπλές ευπάθειες.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Εγκατεστημένη Έκδοση: 5.4.4
Σταθερή Έκδοση: 5.4.39

Επίπτωση:
Η επιτυχής αξιοποίηση του ζητήματος μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να αποκτήσουν ευαίσθητες πληροφορίες μέσω της συνεχούς παροχής δεδομένων με έναν τύπο δεδομένων “int” και να εκτελέσουν αυθαίρετο κώδικα με την συνεχή παροχή δεδομένων με έναν απροσδόκητο τύπο δεδομένων.

Επίπεδο αντίκτυπο: Εφαρμογή

Λύση:
Τύπος λύσης: Επιδιόρθωση κατασκευαστή (VendorFix).
Αναβάθμιση σε php 5.4.39 ή 5.5.23 ή 5.6.7 ή νεότερη έκδοση. Για ενημερώσεις ανατρέξτε στην http://www.php.net

Επηρεάζονται λογισμικά / OS:
Εκδόσεις php πριν 5.4.39, 5.5.x πριν από 5.5.23 και 5.6.x πριν 5.6.7.

Ευπάθεια insight:
Πολλαπλά ελαττώματα οφείλονται σε:

- Η λειτουργία «do_soap_call» σε “ext/soap/soap.c” script στην PHP δεν επιβεβαιώνει ότι το uri κτήσμα είναι συνδεδεμένο.
- Η «SoapClient :: __ call» μέθοδος δέσμης ενεργειών σε “ext/soap/soap.c” script στην PHP δεν ελέγχει αν «__default_headers» είναι ένας πίνακας.
- Ένα ελάττωμα στη λειτουργία «move_uploaded_file» που ενεργοποιείται κατά το χειρισμό NULL bytes.
- Μια κατάσταση υπερχείλισης ακεραίου στη «_zip_cdir_new» λειτουργία στο «zip_dirent.c» script.

Αναφορές:
CVE: CVE-2015-4148, CVE-2015-4147, CVE-2015-2787, CVE-2015-2348, CVE-2015-2331

CERT: CB-K15 / 1437, CB-K15 / 1188, CB-K15 / 1031, CB-K15 / 0966, CB-K15 / 0942, CB-K15 / 0854, CB-K15 / 0809, CB-K15 / 0806, CB-K15 / 0769, CB-K15 / 0757, CB-K15 / 0665, CB-K15 / 0561, CB-K15 / 0482, CB-K15 / 0377, CB-K15 / 0375, CB-K15 / 0372, DFN- CERT-2016-1004, DFN-CERT-2015-1514, DFN-CERT-2015-1252, DFN-CERT-2015-1083, DFN-CERT-2015-1017, DFN-CERT-2015-0989, DFN-CERT- 2015-0900, DFN-CERT-2015-0854, DFN-CERT-2015-0842, DFN-CERT-2015-0809, DFN-CERT-2015-0794, DFN-CERT-2015-0697, DFN-CERT-2015- 0583, DFN-CERT-2015-0505, DFN-CERT-2015 - 0387, DFN-CERT-2015 - 0383, DFN-CERT-2015 - 0382

2.1.17) Κεφαλίδα υπερχείλισης κατά HTTP proxy **(βλ. είκονα 3.1.28)**

Rate -> 7.5 (High)
QOD -> 99%
Port -> 10000 / tcp

Περίληψη:
Ήταν δυνατό να καταρύψει το πληρεξούσιο HTTP στέλνοντας ένα έγκυρο αίτημα με πολύ μεγάλη επικεφαλίδα.
Ένα cracker μπορεί να εκμεταλλευτεί αυτήν την ευπάθεια για να κρασάρει τον διακομιστή μεσολάβησης συνεχώς ή ακόμα και να εκτελέσει αυθαίρετο κώδικα στο σύστημα.

Αποτέλεσμα: Ανίχνευση ευπάθειας:
Ευπάθεια εντοπίστηκε σύμφωνα με την μέθοδο ανίχνευσης ευπαθειών.

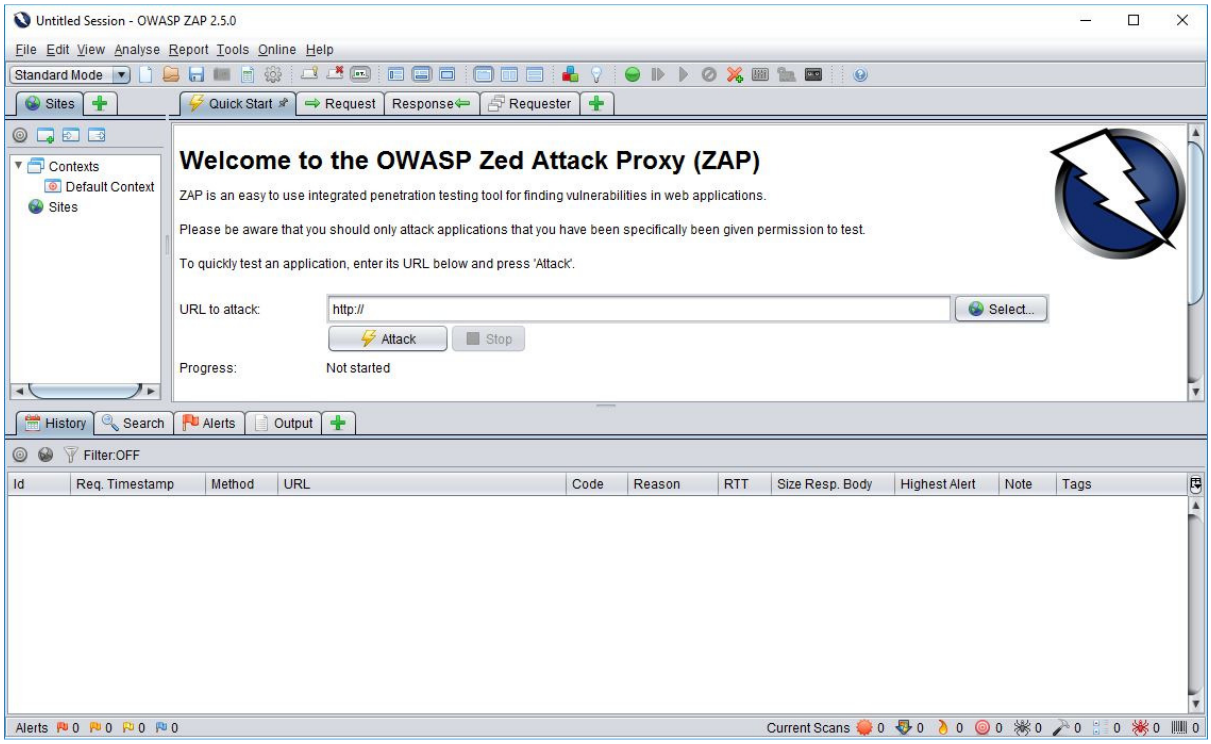
Λύση:
Αναβάθμιση του λογισμικού.

Αναφορές:
CVE: CVE-2002-0133

ΠΡΟΣΦΟΡΑ: 3904, 3905

2.2) OWASP ZAP

Το παρόν λογισμικό είναι γραμμένο στην Java και ανήκει στην κατηγορία του ανοιχτού λογισμικού (open source). Δημιουργήθηκε από την ομάδα του OWASP (Open Web Application Security Project) για την ανάλυση αλλά και την εισχώρηση σε ηλεκτρονικές διευθύνσεις καθώς και εφαρμογές στο πλαίσιο της επιμόρφωσης των δημιουργών τους ώστε να μπορέσουν να τροποποιήσουν τον κωδικά τους αναλόγως. Υποστηρίζει τη δυνατότητα να γράψει ο χρήστης κομμάτια κώδικα (scripts) σε γλώσσες όπως python, ruby ώστε να μπορεί ο οποισδήποτε να τροποποιεί της επιλογές που δίνει το ZAP (Zed Attack Proxy) και να το παραμετροποιεί ανάλογα με τις ανάγκες του. Υποστηρίζεται από όλα τα λογισμικά που κυκλοφορούν (Linux, Windows, Mac OSX κ.α.) και μπορεί να το διαχειριστεί κανείς από το ξεχωριστό του γραφικό περιβάλλον (gui) καθώς και μέσω internet browser (proxy). Μπορεί να πραγματοποιήσει αναλύσεις και επιθέσεις σε διάφορα επίπεδα ανάλογα με τις ανάγκες του χρήστη και μπορεί να παραμετροποιηθεί εύκολα χωρις ιδιαίτερο κόπο. <<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>>



2.2.1) Anti CSRF Tokens Scanner **(βλ. εικονα 3.2.1)**

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Μέτρια
Παράμετρος → Καμία. Προειδοποίηση μόνο.
Επίθεση → Δεν βρέθηκαν Anti-CSRF μάρκες τεχνογνωσίας στο παρακάτω HTML.

Περιγραφή:
Ένα cross-site αίτημα πλαστογραφίας περιλαμβάνει μία επίθεση αναγκάζοντας το θύμα να στείλει μία αίτηση HTTP σε έναν προορισμό-στόχο, χωρίς τη γνώση ή την πρόθεση του, προκειμένου να εκτελέσει μια ενέργεια ως θύμα. Η βασική αιτία είναι η λειτουργία της εφαρμογής, χρησιμοποιώντας προβλέψιμες ενέργειες με έναν επαναλαμβανόμενο τρόπο. Η φύση της CSRF επίθεσης είναι ότι εκμεταλλεύεται την εμπιστοσύνη που μια ιστοσελίδα έχει για ένα χρήστη. Αντίθετα, η επίθεση cross-site scripting (XSS) εκμεταλλεύεται την εμπιστοσύνη που έχει ο χρήστης για μια ιστοσελίδα. Οι XSS, CSRF επιθέσεις δεν είναι κατ' ανάγκη cross-site, αλλά μπορεί να είναι. Ένα cross-site αίτημα πλαστογραφίας είναι επίσης γνωστό ως CSRF, XSRF, one-click attack, session riding, confused deputy και see surf.

CSRF επιθέσεις είναι αποτελεσματικές σε έναν αριθμό καταστάσεων, που περιλαμβάνουν:
- Το θύμα σε μια ενεργή συνεδρία στην περιοχή-στόχο.
- Το θύμα που επικυρώνεται μέσω HTTP εξουσιοδότησης στην περιοχή-στόχο.
- Το θύμα να βρίσκεται στο ίδιο τοπικό δίκτυο με τον στόχο site.

CSRF έχει κυρίως χρησιμοποιηθεί για να εκτελείται μια ενέργεια ενάντια σε ένα σημείο-στόχο, χρησιμοποιώντας τα προνόμια του θύματος, αλλά οι πρόσφατες τεχνικές έχουν ανακαλυφθεί για να αποκαλύπτουν πληροφορίες από την πρόσβαση στην απάντηση. Ο κίνδυνος της αποκάλυψης πληροφοριών αυξάνεται δραματικά όταν η περιοχή-στόχος είναι ευάλωτα σε XSS, επειδή XSS μπορεί να χρησιμοποιηθεί ως πλατφόρμα για CSRF, επιτρέποντας την επίθεση να λειτουργεί μέσα στα όρια της ίδιας πολιτικής προέλευσης.

Λύση: Αρχιτεκτονική και Σχεδιασμός.
Χρησιμοποιήστε ένα πλαίσιο που δεν επιτρέπει να συμβεί αυτού του είδους η αδυναμία ή κατασκευάσματα που κάνουν αυτήν την αδυναμία εύκολο να αποφευχθεί.
Για παράδειγμα, χρησιμοποιήστε τα πακέτα anti-CSRF όπως το OWASP CSRF-Guard.

Εφαρμογή:
Βεβαιώση ότι το αίτημα είναι απαλλαγμένο από τα θέματα cross-site scripting, επειδή οι περισσότερες άμυνες CSRF μπορεί να παρακαμφθούν με τη χρήση ελεγχόμενων scripts από κάποιον εισβολέα.

Προσδιορισμός ιδιαίτερα επικίνδυνων εργασίων. Όταν ο χρήστης εκτελεί μια επικίνδυνη λειτουργία, να στέλνεται μια ξεχωριστή αίτηση επιβεβαίωσης για να εξασφαλιστεί ότι ο χρήστης είναι εξουσιοδοτημένος για την εκτέλεση αυτής της λειτουργίας.
Σημειώνουμε ότι αυτό μπορεί να παρακαμφθεί με τη χρήση XSS.

Χρησιμοποιήστε τον έλεγχο ESAPI Διαχείρισης Συνεδρία.
Ο έλεγχος αυτός περιλαμβάνει μια συνιστώσα για CSRF.

Μην χρησιμοποιείτε τη μέθοδο GET για κάθε αίτημα που πυροδοτεί μια αλλαγή κατάστασης.

2.2.2) Heartbleed OpenSSL Vulnerability (Indicative) **(βλ. εικόνα 3.2.2)**

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Χαμηλή
Αποδεικτικά στοιχεία → OpenSSL / 1.0.1.c

Περιγραφή:
Οι εφαρμογές TLS και DTLS στο OpenSSL 1.0.1 πριν την 1.0.1g δεν χειρίζονται σωστά τα Heartbeat Extension Packets, τα οποία επιτρέπουν στους απομακρυσμένους επιτηθέμενους να αποκτήσουν ευαίσθητες πληροφορίες από τη μνήμη διαδικασίας μέσω δημιουργημένων ρυθμιζόμενων πακέτων που ενεργοποιούνται όταν ενδεχομένως αποκαλυφθούν ευαίσθητες πληροφορίες.

Λύση:
Ενημέρωση για OpenSSL 1.0.1g ή νεότερη έκδοση. Επανέκδοση πιστοποιητικών HTTPS. Αλλαγή στα ασύμμετρα ιδιωτικά κλειδιά και τα κοινά μυστικά κλειδιά, δεδομένου ότι αυτά μπορεί να έχουν παραβιαστεί, χωρίς ενδείξεις συμβιβασμού στα αρχεία καταγραφής του διακομιστή.

2.2.3) Ανασφαλής Component - Apache 2.4.4 **(βλ. εικόνα 3.2.3)**

Κίνδυνος → Υψηλή
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → Apache / 2.4.2 (Win32) OpenSSL / 1.0.1.c PHP / 5.4.4

Περιγραφή:
Με βάση την παθητική ανάλυση της απάντησης, ανασφαλής συστατικό Apache 2.4.2 φαίνεται να είναι σε χρήση.
Την υψηλότερη βαθμολογία σημείωσε η CVSS, για αυτό το προϊόν η έκδοση είναι 7,5.
Συνολικά, σημειώθηκαν 12 τρωτά σημεία.
Μερικές διανομές Linux όπως το Red Hat, απασχολούν την πρακτική της διατήρησης παλαιών αριθμών έκδοσης όταν οι διορθώσεις ασφαλείας είναι "backported".
Αυτές οι περιπτώσεις σημειώνονται ως "False-Positives", οι οποίες θα πρέπει να επαληθεύόνται χειροκίνητα.

Λύση:
Αναβάθμιση από Apache 2.4.2 στην τελευταία σταθερή έκδοση του προϊόντος.
Χρησιμοποιήστε ένα διαχειριστή πακέτων για τη διαχείριση των εγκατεστημένων εκδόσεων των πακέτων λογισμικού.

2.2.4) Ανασφαλής Component - Microsoft IIS 7.5 (βλ. εικόνα 3.2.4)

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → Microsoft-IIS / 7.5

Περιγραφή:
Με βάση την παθητική ανάλυση της απάντησης, ανασφαλής συστατικό Microsoft-IIS 7.5 φαίνεται να είναι σε χρήση.
Υψηλότερη βαθμολογία σημείωσε το CVSS, για αυτό το προϊόν η έκδοση είναι 10.
Συνολικά, παρατηρήθηκαν 5 τρωτά σημεία.
Μερικές διανομές Linux όπως Red Hat απασχολούν την πρακτική της διατήρησης παλαιών αριθμών έκδοσης όταν οι διορθώσεις ασφαλείας είναι "backported".
Αυτές οι περιπτώσεις σημειώνονται ως "False-Positives", οι οποίες θα πρέπει να επαληθεύονται χειροκίνητα.

Λύση:
Αναβάθμιση από τη Microsoft-IIS 7.5 με την τελευταία σταθερή έκδοση του προϊόντος.
Χρησιμοποιήστε ένα διαχειριστή πακέτων για τη διαχείριση των εγκατεστημένων εκδόσεων των πακέτων λογισμικού.

2.2.5) Ανασφαλής Component - OpenSSL 1.0.1.c (βλ. εικόνα 3.2.5)

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → Apache / 2.4.2 (Win32) OpenSSL / 1.0.1.c PHP / 5.4.4

Περιγραφή:
Με βάση την παθητική ανάλυση της απάντησης, ανασφαλής συστατικό OpenSSL 1.0.1c φαίνεται να είναι σε χρήση.
Υψηλότερη βαθμολογία σημείωσε το CVSS, για αυτό το προϊόν η έκδοση είναι 7,5.
Συνολικά, σημειώθηκαν 31 τρωτά σημεία.
Μερικές διανομές Linux όπως Red Hat απασχολούν την πρακτική της διατήρησης παλαιών αριθμών έκδοσης όταν οι διορθώσεις ασφαλείας είναι "backported".
Αυτές οι περιπτώσεις σημειώνονται ως "False-Positives", οι οποίες θα πρέπει να επαληθεύονται χειροκίνητα.

Λύση:
Αναβάθμιση από OpenSSL 1.0.1c στην τελευταία σταθερή έκδοση του προϊόντος.
Χρησιμοποιήστε ένα διαχειριστή πακέτων για τη διαχείριση των εγκατεστημένων εκδόσεων των πακέτων λογισμικού.

2.2.6) Ανασφαλής Component - PHP 5.4.4 (βλ. εικόνα 3.2.6)

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → Apache / 2.4.2 (Win32) OpenSSL / 1.0.1.c PHP / 5.4.4

Περιγραφή:
Με βάση την παθητική ανάλυση της απάντησης, ανασφαλής συστατικό PHP 5.4.4 φαίνεται να είναι σε χρήση.
Υψηλότερη βαθμολογία σημείωσε το CVSS, για αυτό το προϊόν η έκδοση είναι 10.
Συνολικά, σημειώθηκαν 31 τρωτά σημεία.
Μερικές διανομές Linux όπως Red Hat απασχολούν την πρακτική της διατήρησης παλαιών αριθμών έκδοσης όταν οι διορθώσεις ασφαλείας είναι "backported".
Αυτές οι περιπτώσεις σημειώνονται ως "False-Positives", οι οποίες θα πρέπει να επαληθεύονται χειροκίνητα.

Λύση:
Αναβάθμιση από την PHP 5.4.4 στην τελευταία σταθερή έκδοση του προϊόντος.
Χρησιμοποιήστε ένα διαχειριστή πακέτων για τη διαχείριση των εγκατεστημένων εκδόσεων των πακέτων λογισμικού.

2.2.7) Ανασφαλής Component - PHP 5.5.9 (βλ. εικόνα 3.2.7)

Κίνδυνος → Υψηλός
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → PHP / 5.5.9-1 ubuntu 4.17

Περιγραφή:
Με βάση την παθητική ανάλυση της απάντησης, ανασφαλής συστατικό PHP 5.5.9 φαίνεται να είναι σε χρήση.
Υψηλότερη βαθμολογία σημείωσε το CVSS, για αυτό το προϊόν η έκδοση είναι 7,5.
Συνολικά, σημειώθηκαν 24 τρωτά σημεία.
Μερικές διανομές Linux όπως Red Hat απασχολούν την πρακτική της διατήρησης παλαιών αριθμών έκδοσης όταν οι διορθώσεις ασφαλείας είναι "backported".
Αυτές οι περιπτώσεις σημειώνονται ως "False-Positives", οι οποίες θα πρέπει να επαληθεύονται χειροκίνητα.

Λύση:
Αναβάθμιση από την PHP 5.5.9 στην τελευταία σταθερή έκδοση του προϊόντος.
Χρησιμοποιήστε ένα διαχειριστή πακέτων για τη διαχείριση των εγκατεστημένων εκδόσεων των πακέτων λογισμικού.

2.2.8) Backup File Disclosure (βλ. εικόνα 3.2.8)

Κίνδυνος → Μέτριος
Εμπιστοσύνη → Μέτρια

Περιγραφή:
Το αντίγραφο ασφαλείας ενός αρχείου φανερώνεται από τον web server.

Λύση:
Μην επεξεργάζεστε τα “in-situ” αρχεία του web server και επιβεβαιώστε ότι τα αχρείαστα αρχεία (μαζι με τα κρυφά αρχεία) είναι διεγραμμένα από τον web server.

2.2.9) Directory Browsing (βλ. εικόνα 3.2.9)

Κίνδυνος → Μέτριος
Εμπιστοσύνη → Μέτρια
Επίθεση → (Parent Directory)

Περιγραφή:
Είναι δυνατόν να εμφανιστεί ολόκληρος ο κατάλογος (directory). Η εμφάνιση του καταλόγου μπορεί να εμφανίσει κρυμμένα χειρόγραφα (scripts), περιεχόμενα αρχείων, εφεδρικά πηγαία στοιχεία κ.α., τα οποία είναι προσβάσιμα προς ανάγνωση και εμπεριέχουν ευαίσθητες πληροφορίες.

Λύση:
Απενεργοποιήστε την εξερεύνηση του καταλόγου. Αν αυτό απαιτείται, σιγουρευτείται ότι δεν περιέχει ευαίσθητες πληροφορίες.

2.2.10) HTTP Parameter Override (βλ. εικόνα 3.2.10)

Κίνδυνος → Μέτριος
Εμπιστοσύνη → Μέτρια
Αποδεικτικά Στοιχεία → <form class='bootbox-form'>

Περιγραφή:
Απροσδιόριστη φόρμα δράσης με παράμετρο HTTP ενδεχομένως μπορεί να προσπελαστεί. Είναι γνωστό πρόβλημα με τα Java Servlets αλλά και με άλλες πλατφόρμες που είναι και αυτές ευάλωτες.

Λύση:
Όλες οι φόρμες πρέπει να προσδιοριστούν με την μορφή του URL.

2.2.11) Relative Path Conclusion (βλ. εικόνα 3.2.11)

Κίνδυνος → Μέτριος
Εμπιστοσύνη → Μέτρια
Αποδεικτικά στοιχεία → <link rev='made'href='mailto:postmaster@localhost'/>

Περιγραφή:
Ο web server έχει ρυθμιστεί ώστε να εξυπηρετεί τις απαντήσεις σε διφορούμενες διευθύνσεις URL με έναν τρόπο που είναι πιθανό να οδηγήσει σε σύγχυση σχετικά με τη σωστή "σχετική διαδρομή" για τη διεύθυνση URL. Πόροι (CSS, εικόνες, κλπ) είναι επίσης καθορισμένοι στην απάντηση σελίδας χρησιμοποιώντας σχετική, όχι απόλυτη διευθύνση URL. Σε μια επίθεση, αν το πρόγραμμα περιήγησης στο δίκτυο αναλύει την απάντηση "παράλληλου-περιεχομένου" (cross-content) σε έναν ανεκτικό τρόπο, ή μπορεί να παρασυρθεί ώστε να κάνει πιο ανεκτική την ανάλυση της απάντησης "παράλληλου-περιεχομένου" (cross-content), χρησιμοποιώντας τεχνικές όπως διαμόρφωσης (framing), τότε το πρόγραμμα περιήγησης στο δίκτυο μπορεί να ξεγελαστεί ερμηνεύοντας HTML για CSS (ή άλλους τύπους περιεχομένου), που οδηγεί σε μια ευπάθεια XSS.

Άλλες πληφορορίες:
Δεν υπάρχει <base> ετικέτα που να είναι καθορισμένη στη HTML <head> ετικέτα ώστε να καθορίζει το σχετικό URL.
Ο τύπος περιεχομένου "text/html; charset=utf-8" είναι καθορισμένος. Αν το πρόγραμμα περιήγησης έχει αυστηρούς κανόνες, αυτό θα μπορούσε να εμποδίσει παράλληλου-περιεχομένου επιθέσεις από το να επιτύχουν.
Ιδιόρρυθμη λειτουργία εάν εμμέσως ενεργοποιηθεί μέσω της χρήσης ενός παλιού DOCTYPE με το δημόσιο αναγνωριστικό "- // W3C // DTD XHTML 1.0 Strict // EN", επιτρέποντας στο συγκεκριμένο τύπο περιεχομένου να παρακαμφθεί σε ορισμένα προγράμματα περιήγησης στο web.

Λύση:
Web servers και πλαίσια θα πρέπει να ενημερώνονται για να ρυθμιστούν ώστε να μην εξυπηρετούν απαντήσεις σε διφορούμενες διευθύνσεις URL με τέτοιο τρόπο ώστε η σχετική διαδρομή αυτών των διευθύνσεων URL θα μπορούσε να παρερμηνευτεί από τα συστατικά είτε στην πλευρά του πελάτη ή διακομιστή.

Μέσα από την εφαρμογή, η σωστή χρήση του <base> HTML ετικέτας στην απόκριση HTTP θα προσδιορίζει σαφώς τη βάση URL για όλες τις σχετικές διευθύνσεις URL στο έγγραφο.
Χρησιμοποιήστε την "Content-Type" κεφαλίδα απόκρισης HTTP για να γίνει πιο σκληρό σε έναν εισβολέα και να αναγκάσει το πρόγραμμα περιήγησης για λανθασμένη ερμήνευση του τύπου του περιεχομένου της απάντησης.
Χρησιμοποιήστε την "X-Content-Type-Επιλογές: nosniff" κεφαλίδα απόκρισης HTTP για την πρόληψη του web browser από το "sniffing" τον τύπο περιεχομένου της απάντησης.
Χρησιμοποιήστε ένα σύγχρονο DOCTYPE όπως "<! DOCTYPE html>" για να αποφευχθεί η σελίδα από το να αποδίδεται στο πρόγραμμα περιήγησης web χρησιμοποιώντας "Quirks Mode", δεδομένου ότι αυτό έχει ως αποτέλεσμα τον τύπο περιεχομένου που αγνοούνται από το πρόγραμμα περιήγησης στο web.
Καθορίστε την κεφαλίδα απόκρισης HTTP "X-Frame-Options" για την πρόληψη “Quirks Mode” από το να είναι ενεργοποιημένα στο πρόγραμμα περιήγησης web χρησιμοποιώντας τη διαμόρφωση επιθέσεις.

2.2.12) X-Frame-Options Header Not Set **(βλ. εικόνα 3.2.12)**

Κίνδυνος → Μέτριος
Εμπιστοσύνη → Μέτρια

Περιγραφή:
Η κεφαλίδα X-Frame-Options δεν περιλαμβάνεται στην HTTP απάντηση ώστε να προστατευτεί εναντίον “ClickJacking” επιθέσεων.

Άλλες πληροφορίες:
Σε πολλές περιπτώσεις ο ανιχνευτής δεν θα ειδοποιήσει τον χρήστη ή το server με λανθασμένες απαντήσεις.

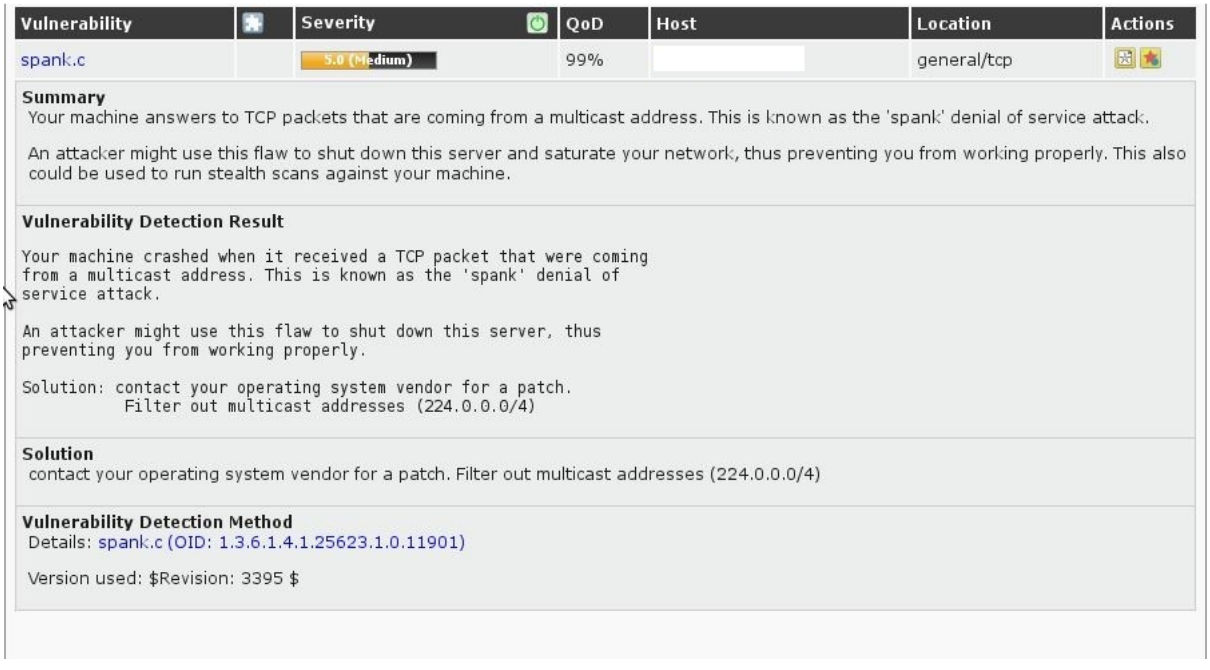
Λύση:
Τα περισσότερα προγράμματα περιήγησης υποστηρίζουν X-Frame-Options HTTP κεφαλίδες. Επιβεβαιώστε ότι είναι ρυθμισμένες όλες οι διαδικτυακές σελίδες, και αν επιστρέφουν από την ηλεκτρονική σελίδα, τότε θα θέλετε να χρησιμοποιήσετε SAMEORIGIN, ειδάλλως μην περιμένετε ότι η ηλεκτρονική σελίδα θα ενοχοποιηθεί.

3) Εικόνες

3.1) OpenVas

3.1.1) Header overflow against HTTP proxy

3.1.2) spank.c



3.1.3) OpenSSL Multiple Vulnerabilities - 02 May16 (Wndows)

Vulnerability	Severity	QoD	Host	Location	Actions
OpenSSL Multiple Vulnerabilities-02 May16 (Windows)	10.0 (High)	80%		8080/tcp	

Summary
This host is running OpenSSL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.1c
Fixed version:     1.0.1o
```

Impact
Successful exploitation will allow a remote attacker to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) condition.

Impact Level: System/Application

Solution
Solution type: VendorFix

Upgrade to OpenSSL 1.0.1o or 1.0.2c or later. For updates refer to https://www.openssl.org

Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1o and 1.0.2 before 1.0.2c on Windows.

Vulnerability Insight
The flaw exists as the ASN.1 parser (specifically, d2i_ASN1_TYPE) can misinterpret a large universal tag as a negative zero value and if an application deserializes untrusted ASN.1 structures containing an ANY field, and later reserializes them, it can trigger an out-of-bounds write.

3.1.4) OpenSSL Multiple Vulnerabilities - 02 May16 (Wndows) 2

Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1o and 1.0.2 before 1.0.2c on Windows.

Vulnerability Insight
The flaw exists as the ASN.1 parser (specifically, d2i_ASN1_TYPE) can misinterpret a large universal tag as a negative zero value and if an application deserializes untrusted ASN.1 structures containing an ANY field, and later reserializes them, it can trigger an out-of-bounds write.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: OpenSSL Multiple Vulnerabilities-02 May16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807816)

Version used: $Revision: 3337 $

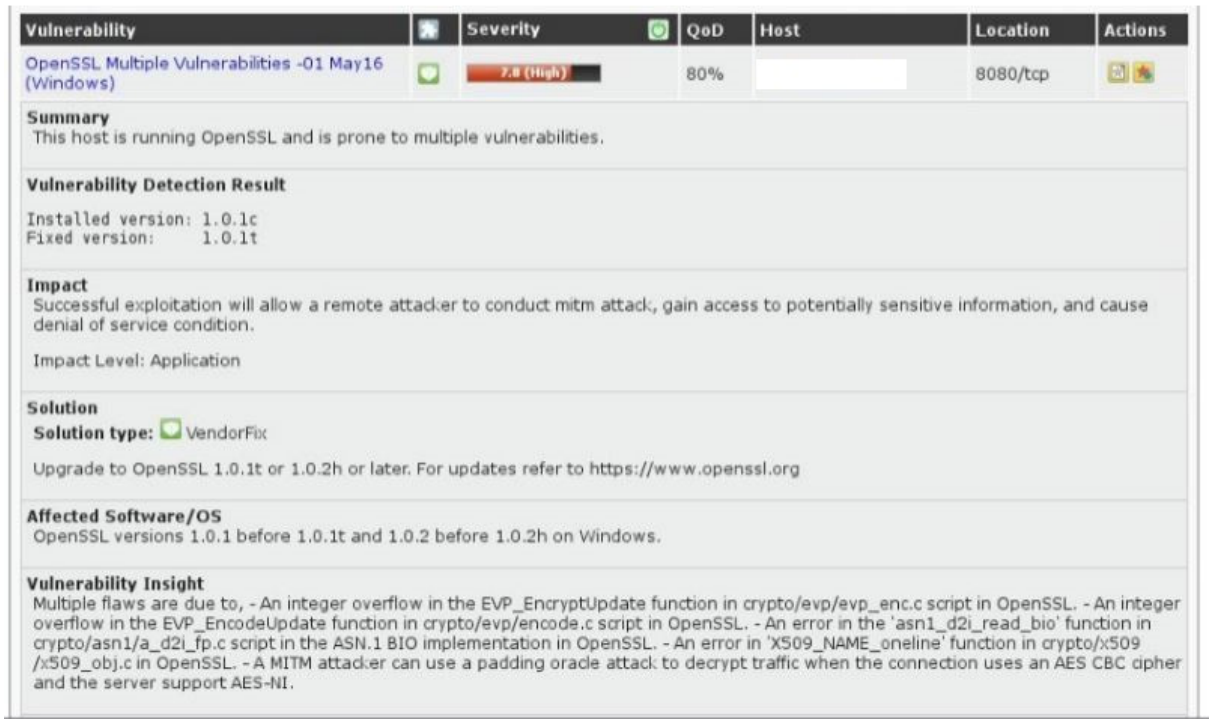
References

CVE: CVE-2016-2108

CERT: DFN-CERT-2016-1401 , DFN-CERT-2016-1160 , DFN-CERT-2016-1103 , DFN-CERT-2016-1092 , DFN-CERT-2016-1091 , DFN-CERT-2016-1026 , DFN-CERT-2016-0867 , DFN-CERT-2016-0815 , DFN-CERT-2016-0765 , DFN-CERT-2016-0702

Other: https://www.openssl.org/news/secadv/20160503.txt

3.1.5) OpenSSL Multiple Vulnerabilities - 01 May16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
OpenSSL Multiple Vulnerabilities -01 May16 (Windows)	7.8 (High)	80%		8080/tcp	

Summary
This host is running OpenSSL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.1c
Fixed version:     1.0.1t
```

Impact
Successful exploitation will allow a remote attacker to conduct mitm attack, gain access to potentially sensitive information, and cause denial of service condition.

Impact Level: Application

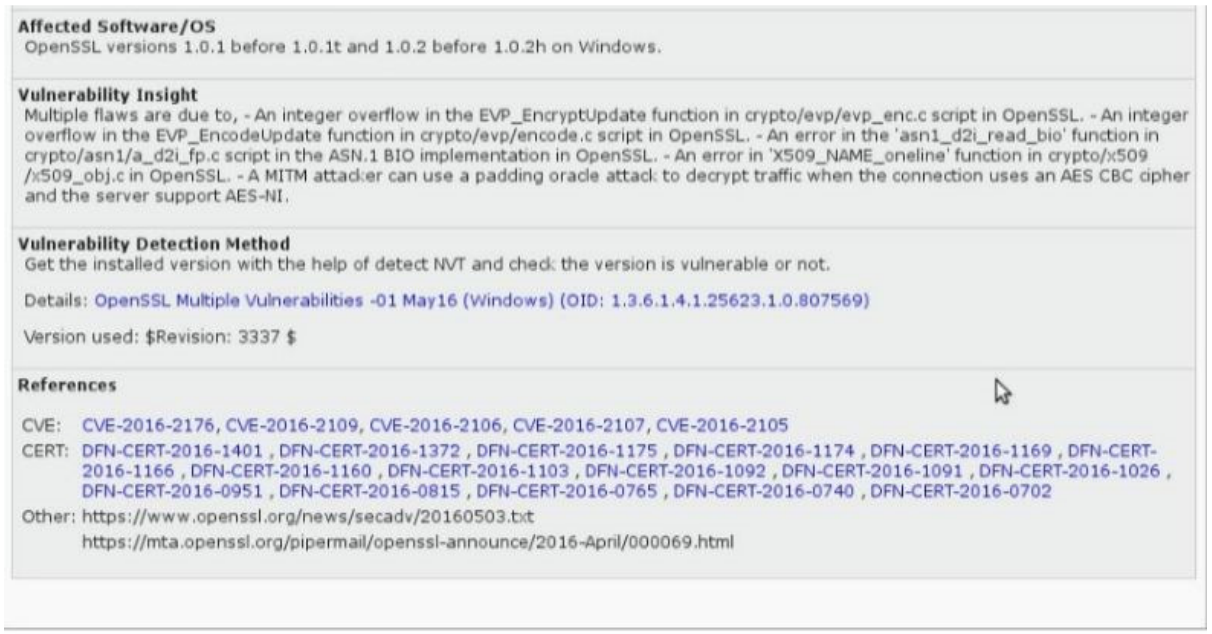
Solution
Solution type: VendorFix

Upgrade to OpenSSL 1.0.1t or 1.0.2h or later. For updates refer to https://www.openssl.org

Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1t and 1.0.2 before 1.0.2h on Windows.

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c script in OpenSSL. - An integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c script in OpenSSL. - An error in the 'asn1_d2i_read_bio' function in crypto/asn1/a_d2i_fp.c script in the ASN.1 BIO implementation in OpenSSL. - An error in 'X509_NAME_oneline' function in crypto/x509 /x509_obj.c in OpenSSL. - A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI.

3.1.6) OpenSSL Multiple Vulnerabilities -01 May16 (Windows) 2



Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1t and 1.0.2 before 1.0.2h on Windows.

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c script in OpenSSL. - An integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c script in OpenSSL. - An error in the 'asn1_d2i_read_bio' function in crypto/asn1/a_d2i_fp.c script in the ASN.1 BIO implementation in OpenSSL. - An error in 'X509_NAME_oneline' function in crypto/x509 /x509_obj.c in OpenSSL. - A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: OpenSSL Multiple Vulnerabilities -01 May16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807569)

Version used: $Revision: 3337 $

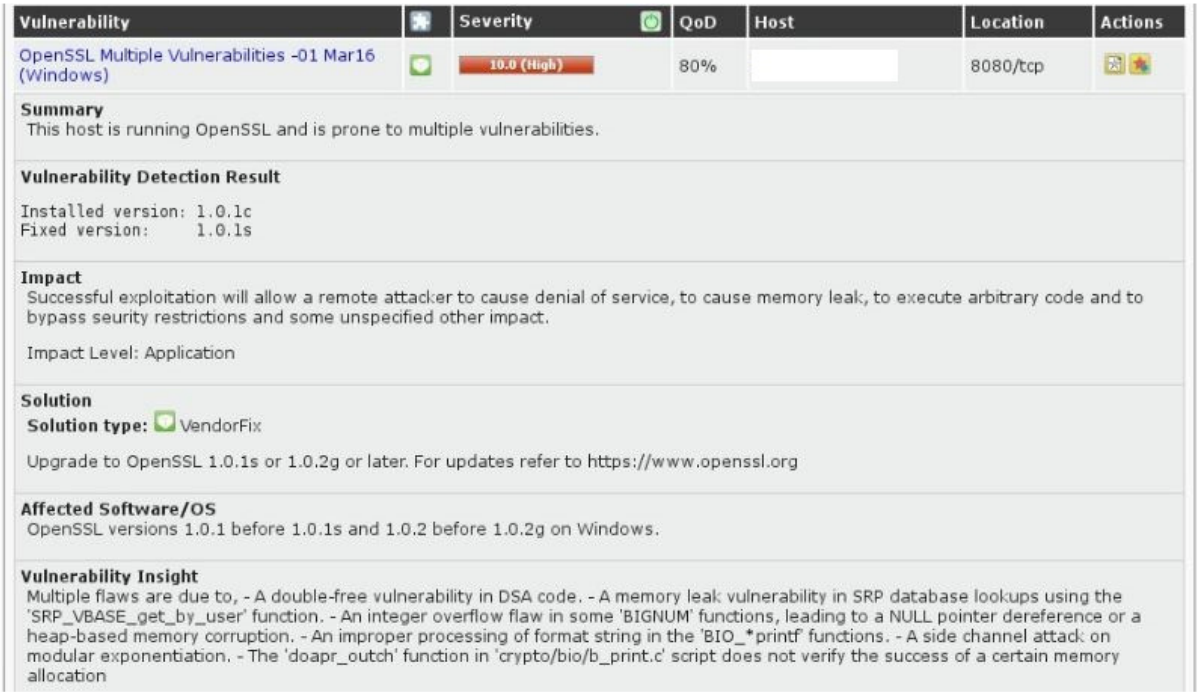
References

CVE: CVE-2016-2176, CVE-2016-2109, CVE-2016-2106, CVE-2016-2107, CVE-2016-2105

CERT: DFN-CERT-2016-1401 , DFN-CERT-2016-1372 , DFN-CERT-2016-1175 , DFN-CERT-2016-1174 , DFN-CERT-2016-1169 , DFN-CERT-2016-1166 , DFN-CERT-2016-1160 , DFN-CERT-2016-1103 , DFN-CERT-2016-1092 , DFN-CERT-2016-1091 , DFN-CERT-2016-1026 , DFN-CERT-2016-0951 , DFN-CERT-2016-0815 , DFN-CERT-2016-0765 , DFN-CERT-2016-0740 , DFN-CERT-2016-0702

Other: https://www.openssl.org/news/secadv/20160503.txt
https://mta.openssl.org/pipermail/openssl-announce/2016-April/000069.html

3.1.7) OpenSSL Multiple Vunerabilities - 01 May16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
OpenSSL Multiple Vulnerabilities -01 Mar16 (Windows)	10.0 (High)	80%		8080/tcp	

Summary
This host is running OpenSSL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.1c
Fixed version:     1.0.1s
```

Impact
Successful exploitation will allow a remote attacker to cause denial of service, to cause memory leak, to execute arbitrary code and to bypass seurity restrictions and some unspecified other impact.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to OpenSSL 1.0.1s or 1.0.2g or later. For updates refer to https://www.openssl.org

Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g on Windows.

Vulnerability Insight
Multiple flaws are due to, - A double-free vulnerability in DSA code. - A memory leak vulnerability in SRP database lookups using the 'SRP_VBASE_get_by_user' function. - An integer overflow flaw in some 'BIGNUM' functions, leading to a NULL pointer dereference or a heap-based memory corruption. - An improper processing of format string in the 'BIO_*printf' functions. - A side channel attack on modular exponentiation. - The 'doapr_outch' function in 'crypto/bio/b_print.c' script does not verify the success of a certain memory allocation

3.1.8) OpenSSL Multiple Vunerabilities - 01 May16 (Windows) 2

Affected Software/OS
OpenSSL versions 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g on Windows.

Vulnerability Insight
Multiple flaws are due to, - A double-free vulnerability in DSA code. - A memory leak vulnerability in SRP database lookups using the 'SRP_VBASE_get_by_user' function. - An integer overflow flaw in some 'BIGNUM' functions, leading to a NULL pointer dereference or a heap-based memory corruption. - An improper processing of format string in the 'BIO_*printf' functions. - A side channel attack on modular exponentiation. - The 'doapr_outch' function in 'crypto/bio/b_print.c' script does not verify the success of a certain memory allocation

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: OpenSSL Multiple Vulnerabilities -01 Mar16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807097)

Version used: $Revision: 2849 $

References

CVE: CVE-2016-0705, CVE-2016-0798, CVE-2016-0797, CVE-2016-0799, CVE-2016-0702, CVE-2016-2842

CERT: DFN-CERT-2016-1401 , DFN-CERT-2016-1389 , DFN-CERT-2016-1245 , DFN-CERT-2016-1175 , DFN-CERT-2016-1174 , DFN-CERT-2016-1103 , DFN-CERT-2016-1026 , DFN-CERT-2016-0951 , DFN-CERT-2016-0890 , DFN-CERT-2016-0841 , DFN-CERT-2016-0815 , DFN-CERT-2016-0803 , DFN-CERT-2016-0789 , DFN-CERT-2016-0765 , DFN-CERT-2016-0699 , DFN-CERT-2016-0698 , DFN-CERT-2016-0644 , DFN-CERT-2016-0499 , DFN-CERT-2016-0496 , DFN-CERT-2016-0465 , DFN-CERT-2016-0459 , DFN-CERT-2016-0453 , DFN-CERT-2016-0403 , DFN-CERT-2016-0388 , DFN-CERT-2016-0360 , DFN-CERT-2016-0359 , DFN-CERT-2016-0357

Other: https://www.openssl.org/news/secadv/20160301.txt

3.1.9) P-smash DOS (ICMP 9 flood)

Vulnerability	Severity	QoD	Host	Location	Actions
p-smash DoS (ICMP 9 flood)	7.8 (High)	99%		general/tcp	

Summary
It was possible to crash the remote machine by flooding it with ICMP type 9 packets.

A cracker may use this attack to make this host crash continuously, preventing you from working properly.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

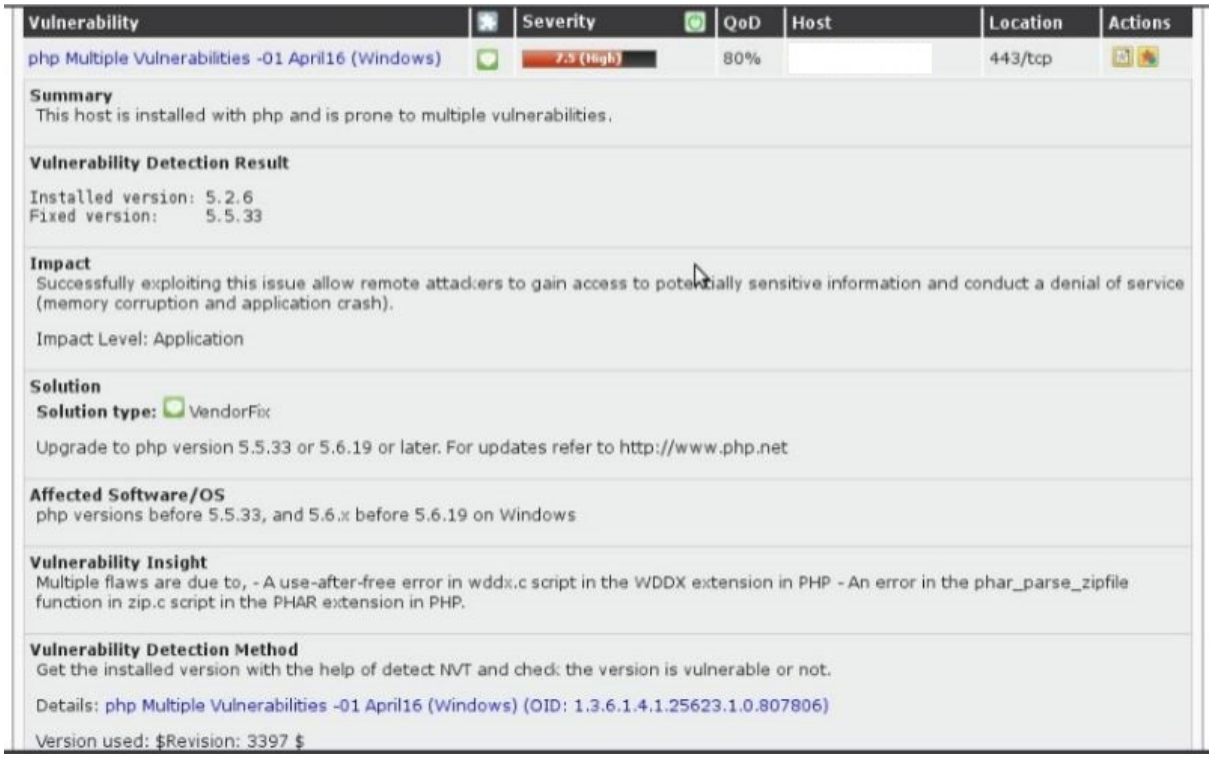
Solution
upgrade your Windows 9x operating system or change it.

Reference : http://support.microsoft.com/default.aspx?scid=KB en-us q216141

Vulnerability Detection Method
Details: p-smash DoS (ICMP 9 flood) (OID: 1.3.6.1.4.1.25623.1.0.11024)

Version used: $Revision: 3395 $

3.1.10) Php Multiple Vulnerabilities - 01 April16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php Multiple Vulnerabilities -01 April16 (Windows)	7.5 (High)	80%		443/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.2.6
Fixed version:     5.5.33
```

Impact
Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to php version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.5.33, and 5.6.x before 5.6.19 on Windows

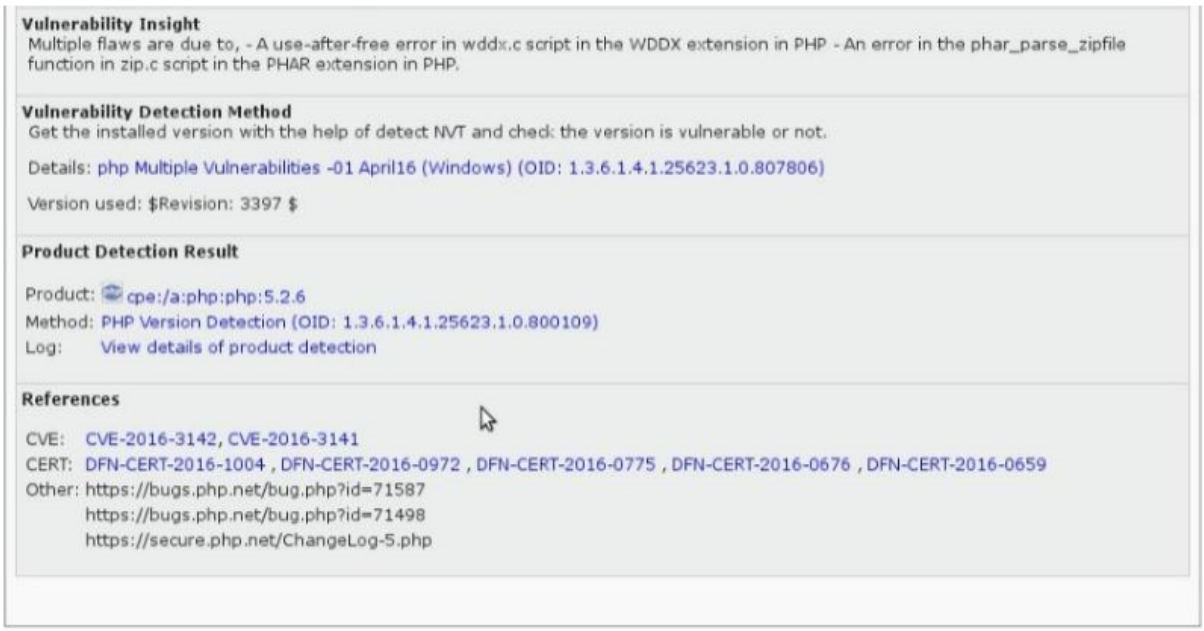
Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Vulnerabilities -01 April16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807806)

Version used: $Revision: 3397 $

3.1.11) Php Multiple Vulnerabilities - 01 April16 (Windows) 2



Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Vulnerabilities -01 April16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807806)

Version used: $Revision: 3397 $

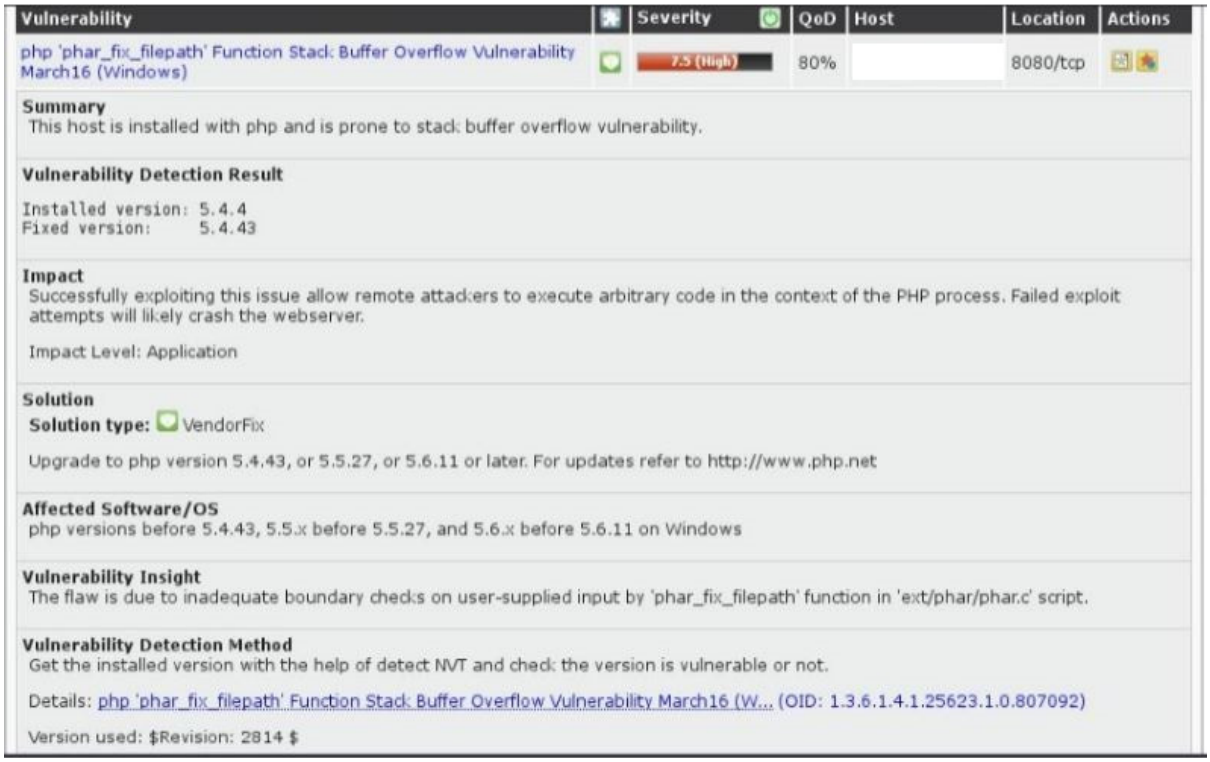
Product Detection Result

Product: cpe:/a:php:php:5.2.6
Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)
Log: View details of product detection

References

CVE: CVE-2016-3142, CVE-2016-3141
CERT: DFN-CERT-2016-1004 , DFN-CERT-2016-0972 , DFN-CERT-2016-0775 , DFN-CERT-2016-0676 , DFN-CERT-2016-0659
Other: https://bugs.php.net/bug.php?id=71587
https://bugs.php.net/bug.php?id=71498
https://secure.php.net/ChangeLog-5.php

3.1.12) Php 'phar_fix_filepath' FunctionStack Buffer Overflow Vulnerability March16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability March16 (Windows)	7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result

Installed version: 5.4.4
Fixed version: 5.4.43

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to php version 5.4.43, or 5.5.27, or 5.6.11 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Windows

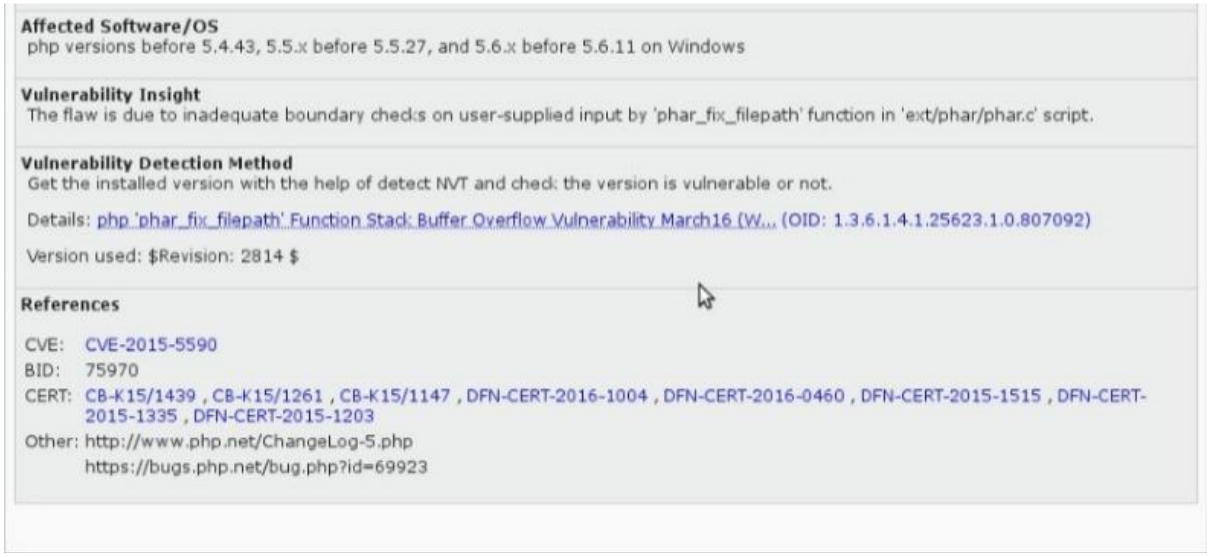
Vulnerability Insight
The flaw is due to inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability March16 (W... (OID: 1.3.6.1.4.1.25623.1.0.807092)

Version used: $Revision: 2814 $

3.1.13) Php ‘phar_fix_filepath’ FunctionStack Buffer Overflow Vulnerability March16 (Windows) 2



Affected Software/OS
php versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Windows

Vulnerability Insight
The flaw is due to inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

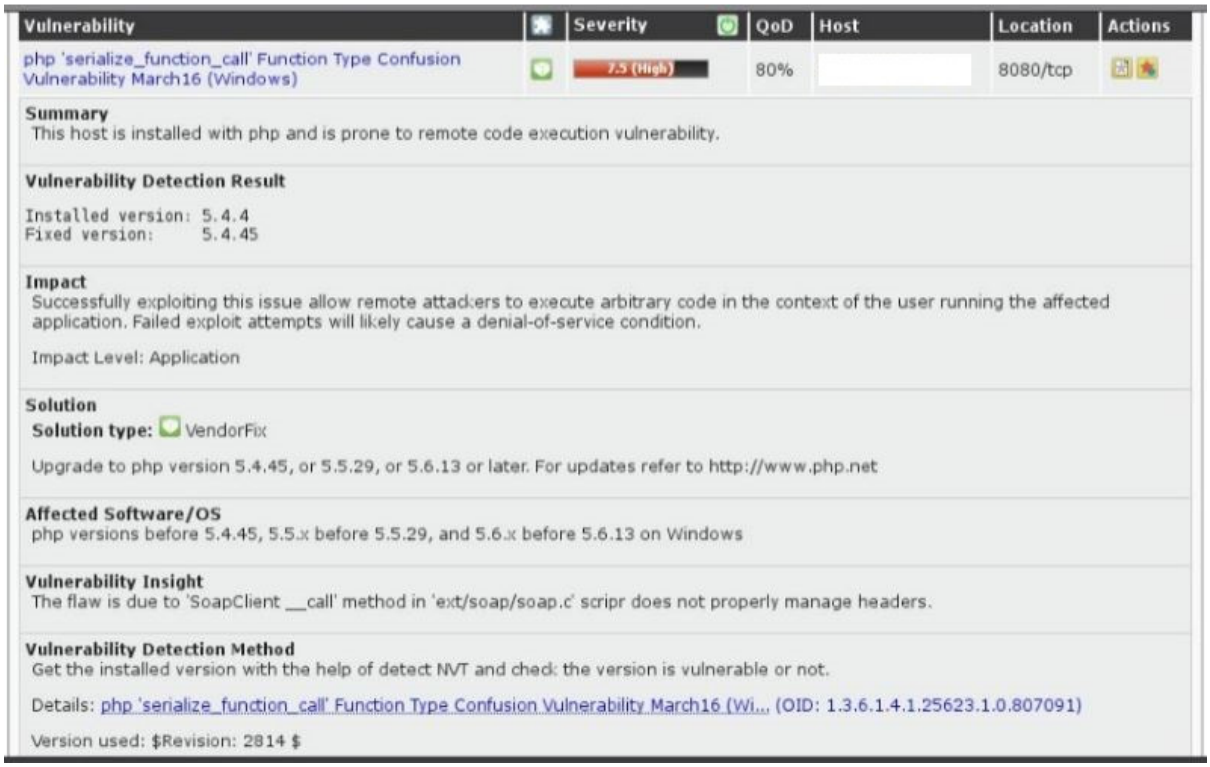
Details: php 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability March16 (W... (OID: 1.3.6.1.4.1.25623.1.0.807092)

Version used: $Revision: 2814 $

References

CVE: CVE-2015-5590
BID: 75970
CERT: CB-K15/1439 , CB-K15/1261 , CB-K15/1147 , DFN-CERT-2016-1004 , DFN-CERT-2016-0460 , DFN-CERT-2015-1515 , DFN-CERT-2015-1335 , DFN-CERT-2015-1203
Other: http://www.php.net/ChangeLog-5.php
https://bugs.php.net/bug.php?id=69923

3.1.14) Php ‘serialize_function_call’ Function Type Confusion Vulnerability March16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php 'serialize_function_call' Function Type Confusion Vulnerability March16 (Windows)	7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.4
Fixed version:     5.4.45
```

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to php version 5.4.45, or 5.5.29, or 5.6.13 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Windows

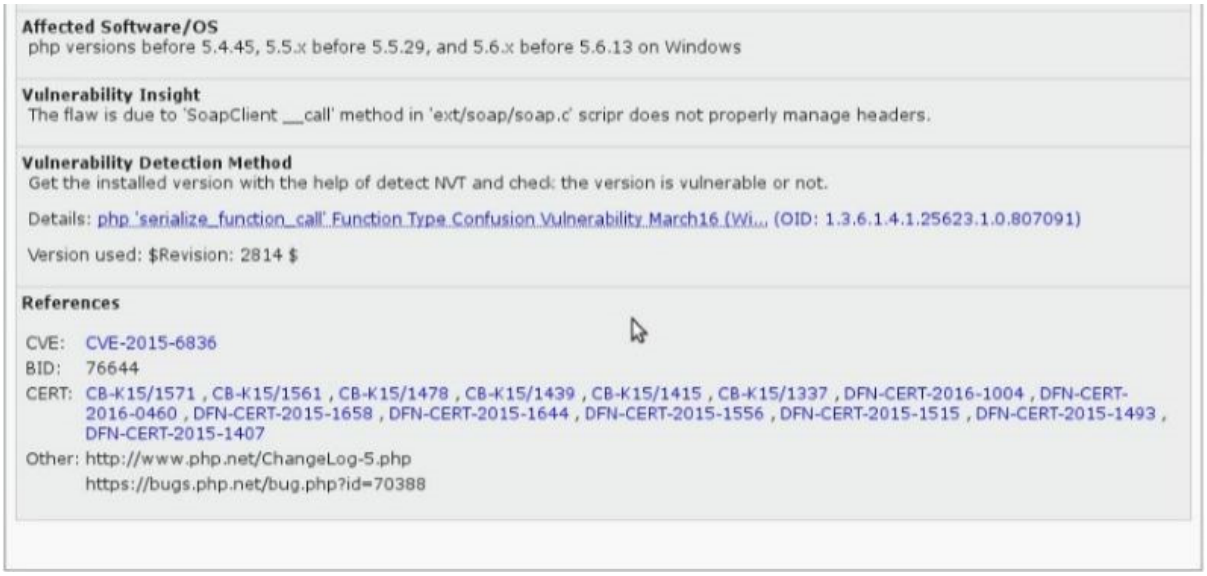
Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php 'serialize_function_call' Function Type Confusion Vulnerability March16 (Wi... (OID: 1.3.6.1.4.1.25623.1.0.807091)

Version used: $Revision: 2814 $

3.1.15) Php ‘serialize_function_call’ Function Type Confusion Vulnerability March16 (Windows) 2



Affected Software/OS
php versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Windows

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and chedi the version is vulnerable or not.

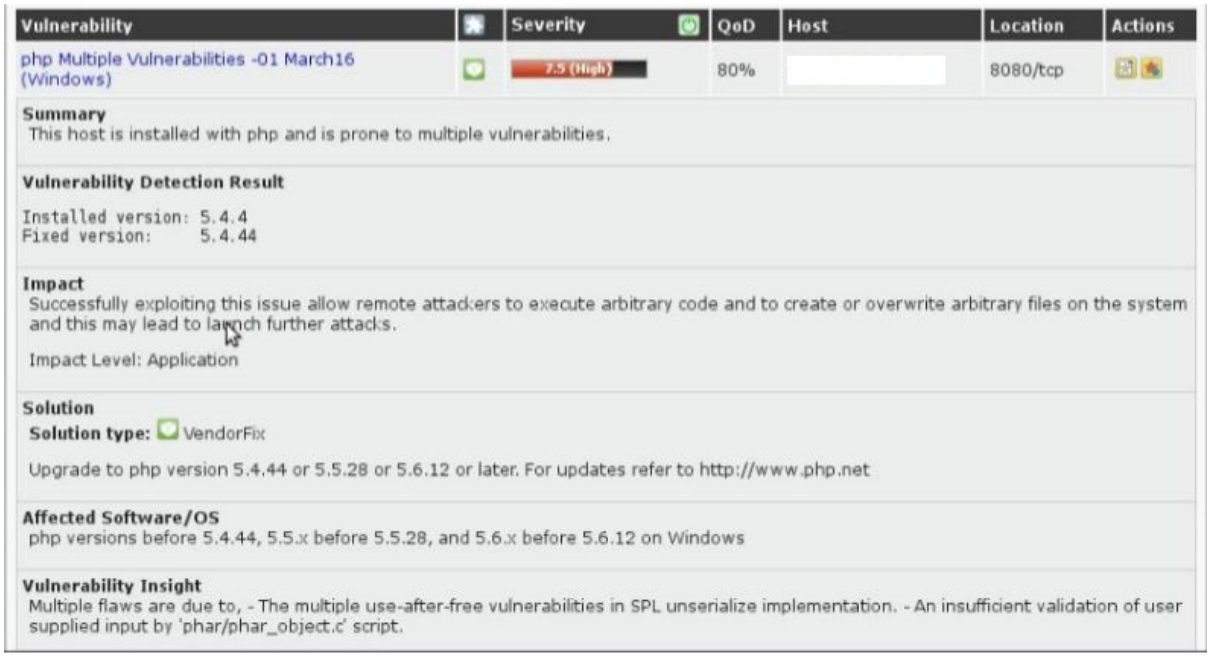
Details: php 'serialize_function_call' Function Type Confusion Vulnerability March16 (Wi... (OID: 1.3.6.1.4.1.25623.1.0.807091)

Version used: $Revision: 2814 $

References

CVE: CVE-2015-6836
BID: 76644
CERT: CB-K15/1571 , CB-K15/1561 , CB-K15/1478 , CB-K15/1439 , CB-K15/1415 , CB-K15/1337 , DFN-CERT-2016-1004 , DFN-CERT-2016-0460 , DFN-CERT-2015-1658 , DFN-CERT-2015-1644 , DFN-CERT-2015-1556 , DFN-CERT-2015-1515 , DFN-CERT-2015-1493 , DFN-CERT-2015-1407
Other: http://www.php.net/ChangeLog-5.php
https://bugs.php.net/bug.php?id=70388

3.1.16) Php Multiple Vulnerabilities - 01 March16 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php Multiple Vulnerabilities -01 March16 (Windows)	7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.4
Fixed version:     5.4.44
```

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks.

Impact Level: Application

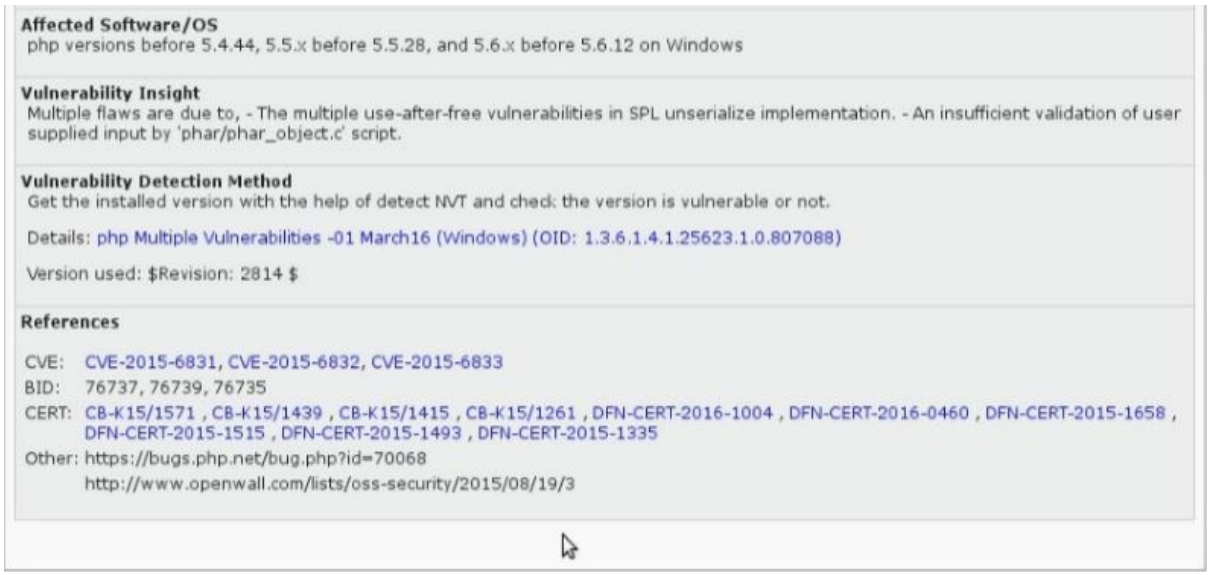
Solution
Solution type: VendorFix

Upgrade to php version 5.4.44 or 5.5.28 or 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Windows

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script.

3.1.17) Php Multiple Vulnerabilities - 01 March16 (Windows) 2



Affected Software/OS
php versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Windows

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

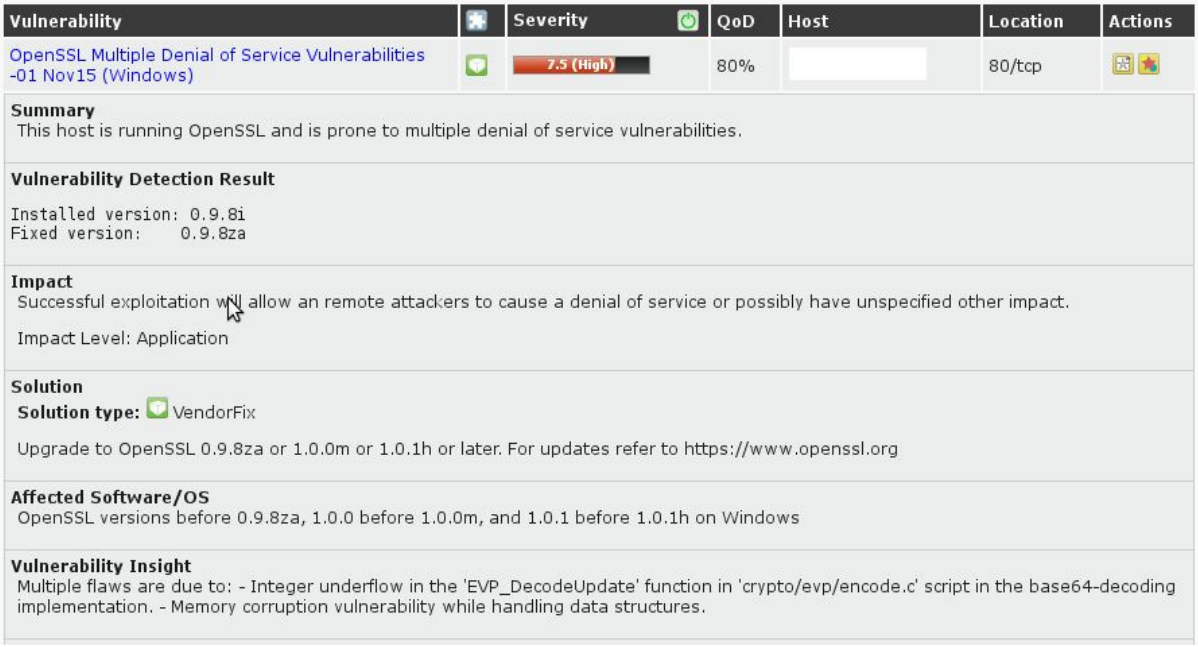
Details: php Multiple Vulnerabilities -01 March16 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.807088)

Version used: $Revision: 2814 $

References

CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
BID: 76737, 76739, 76735
CERT: CB-K15/1571 , CB-K15/1439 , CB-K15/1415 , CB-K15/1261 , DFN-CERT-2016-1004 , DFN-CERT-2016-0460 , DFN-CERT-2015-1658 , DFN-CERT-2015-1515 , DFN-CERT-2015-1493 , DFN-CERT-2015-1335
Other: https://bugs.php.net/bug.php?id=70068
http://www.openwall.com/lists/oss-security/2015/08/19/3

3.1.18) OpenSSL Multiple Denial Of Service Vulneravilities - 01 Nov15 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
OpenSSL Multiple Denial of Service Vulnerabilities -01 Nov15 (Windows)	7.5 (High)	80%		80/tcp	

Summary
This host is running OpenSSL and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 0.9.8i
Fixed version:     0.9.8za
```

Impact
Successful exploitation will allow an remote attackers to cause a denial of service or possibly have unspecified other impact.

Impact Level: Application

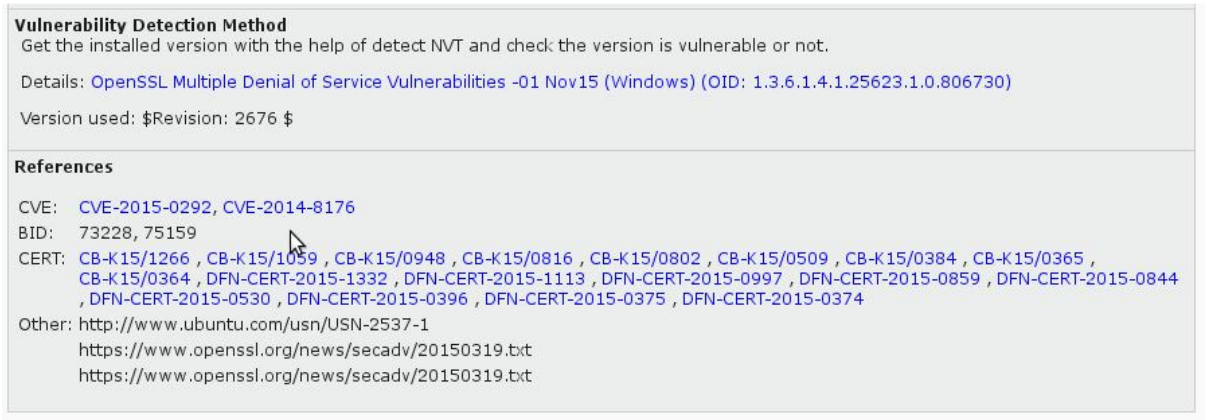
Solution
Solution type: VendorFix

Upgrade to OpenSSL 0.9.8za or 1.0.0m or 1.0.1h or later. For updates refer to https://www.openssl.org

Affected Software/OS
OpenSSL versions before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h on Windows

Vulnerability Insight
Multiple flaws are due to: - Integer underflow in the 'EVP_DecodeUpdate' function in 'crypto/evp/encode.c' script in the base64-decoding implementation. - Memory corruption vulnerability while handling data structures.

3.1.19) OpenSSL Multiple Denial Of Service Vulneravilities - 01 Nov15 (Windows) 2



Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: OpenSSL Multiple Denial of Service Vulnerabilities -01 Nov15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.806730)

Version used: $Revision: 2676 $

References

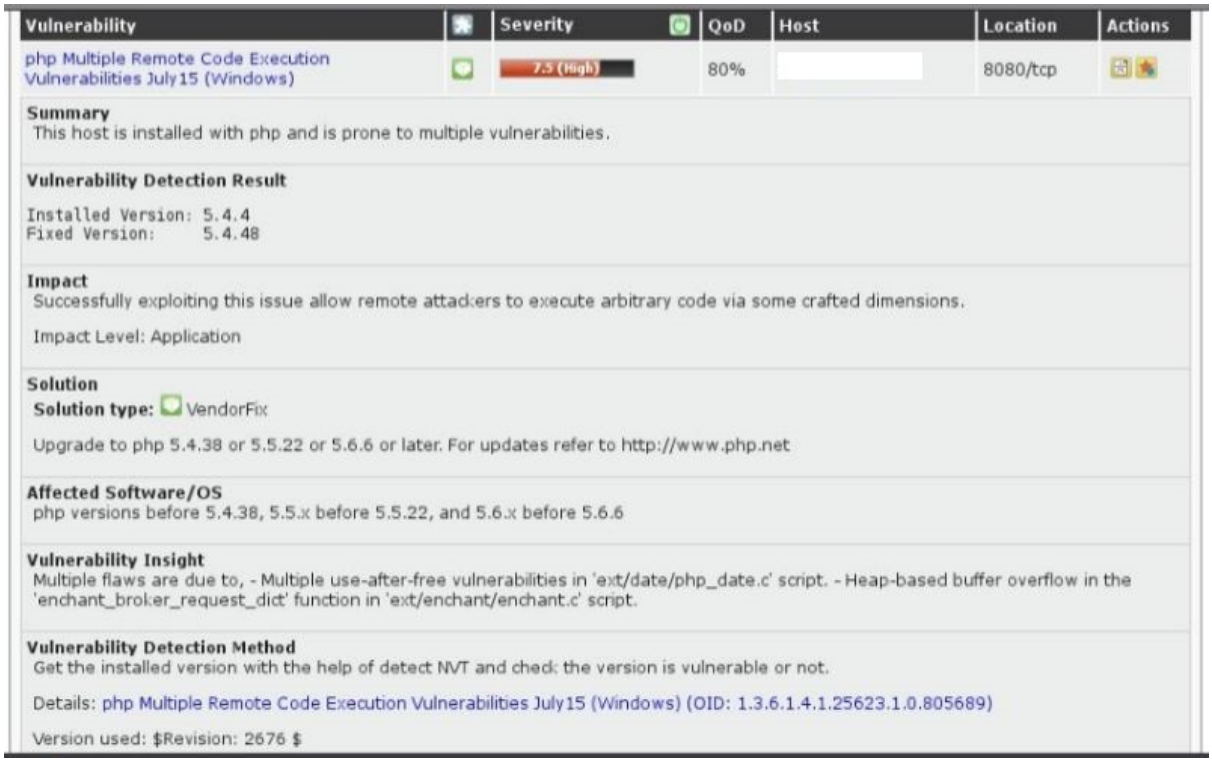
CVE: CVE-2015-0292, CVE-2014-8176

BID: 73228, 75159

CERT: CB-K15/1266 , CB-K15/1059 , CB-K15/0948 , CB-K15/0816 , CB-K15/0802 , CB-K15/0509 , CB-K15/0384 , CB-K15/0365 , CB-K15/0364 , DFN-CERT-2015-1332 , DFN-CERT-2015-1113 , DFN-CERT-2015-0997 , DFN-CERT-2015-0859 , DFN-CERT-2015-0844 , DFN-CERT-2015-0530 , DFN-CERT-2015-0396 , DFN-CERT-2015-0375 , DFN-CERT-2015-0374

Other: http://www.ubuntu.com/usn/USN-2537-1
https://www.openssl.org/news/secadv/20150319.txt
https://www.openssl.org/news/secadv/20150319.txt

3.1.20) Php Multiple Remote Code Execution Vulnerabilities July15 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php Multiple Remote Code Execution Vulnerabilities July15 (Windows)	7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.4
Fixed Version:     5.4.48
```

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to php 5.4.38 or 5.5.22 or 5.6.6 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6

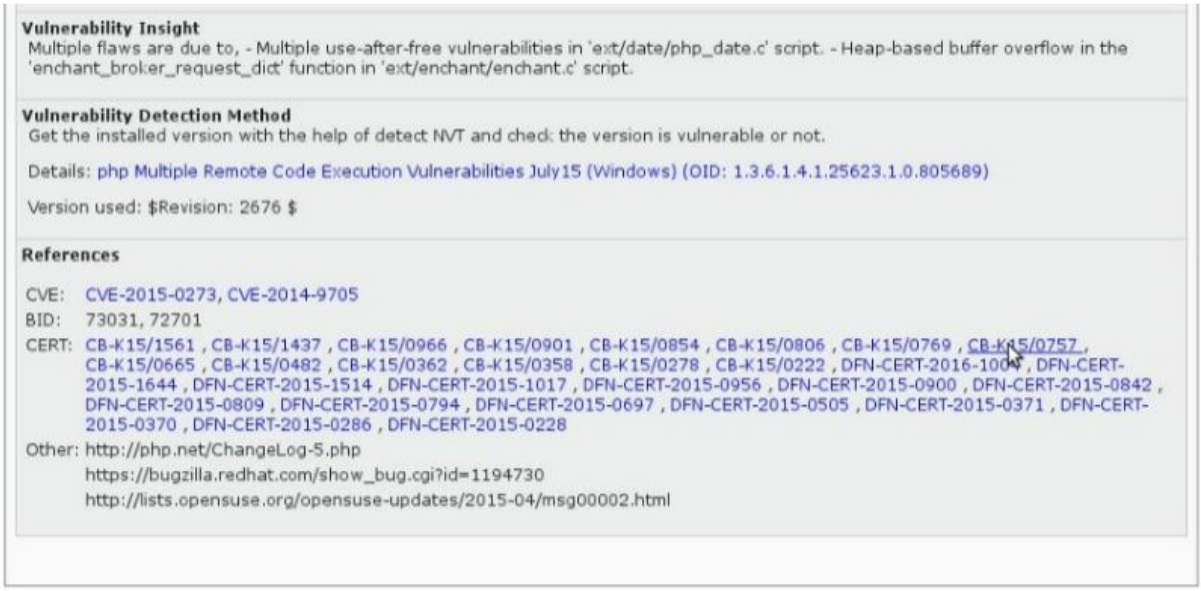
Vulnerability Insight
Multiple flaws are due to, - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Remote Code Execution Vulnerabilities July15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.805689)

Version used: $Revision: 2676 $

3.1.21) Php Multiple Remote Code Execution Vulnerabilities July15 (Windows) 2



Vulnerability Insight
Multiple flaws are due to, - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and chedi the version is vulnerable or not.

Details: php Multiple Remote Code Execution Vulnerabilities July15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.805689)

Version used: $Revision: 2676 $

References

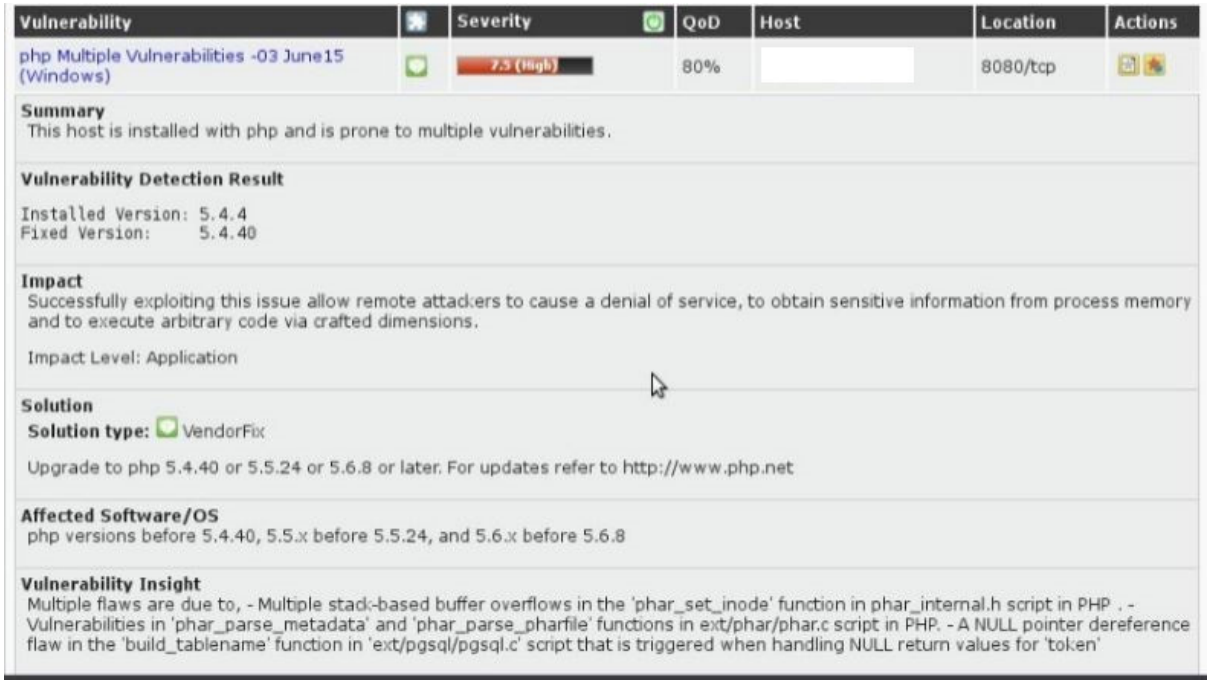
CVE: CVE-2015-0273, CVE-2014-9705

BID: 73031, 72701

CERT: CB-K15/1561 , CB-K15/1437 , CB-K15/0966 , CB-K15/0901 , CB-K15/0854 , CB-K15/0806 , CB-K15/0769 , CB-K15/0757 , CB-K15/0665 , CB-K15/0482 , CB-K15/0362 , CB-K15/0358 , CB-K15/0278 , CB-K15/0222 , DFN-CERT-2016-1004 , DFN-CERT-2015-1644 , DFN-CERT-2015-1514 , DFN-CERT-2015-1017 , DFN-CERT-2015-0956 , DFN-CERT-2015-0900 , DFN-CERT-2015-0842 , DFN-CERT-2015-0809 , DFN-CERT-2015-0794 , DFN-CERT-2015-0697 , DFN-CERT-2015-0505 , DFN-CERT-2015-0371 , DFN-CERT-2015-0370 , DFN-CERT-2015-0286 , DFN-CERT-2015-0228

Other: http://php.net/ChangeLog-5.php
https://bugzilla.redhat.com/show_bug.cgi?id=1194730
http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html

3.1.22) Php Multiple Vulnerabilities - 03 June15 (Windows) 1



Vulnerability		Severity	QoD	Host	Location	Actions
php Multiple Vulnerabilities -03 June15 (Windows)		7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.4
Fixed Version:     5.4.40
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to php 5.4.40 or 5.5.24 or 5.6.8 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8

Vulnerability Insight
Multiple flaws are due to, - Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP . - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'

3.1.23) Php Multiple Vulnerabilities - 03 June15 (Windows) 2

Vulnerability Insight
Multiple flaws are due to, - Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP . - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Vulnerabilities -03 June15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.805656)

Version used: $Revision: 2676 $

References

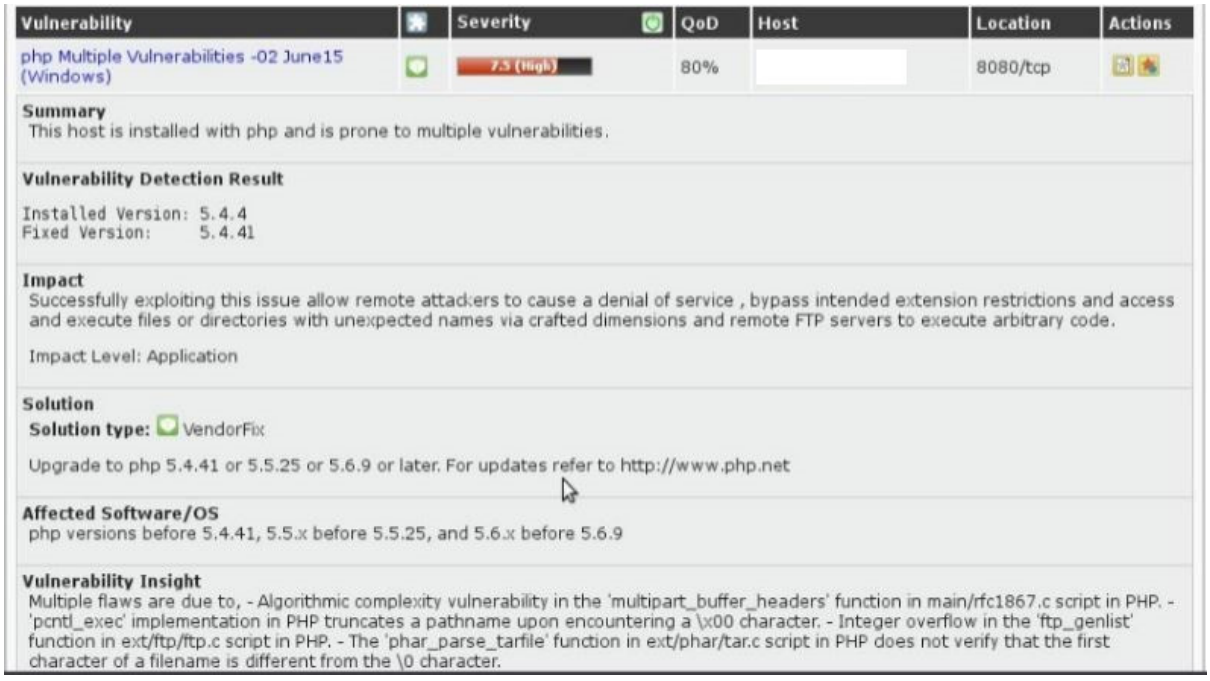
CVE: CVE-2015-3329, CVE-2015-3307, CVE-2015-2783, CVE-2015-1352

BID: 74240, 74239, 74703

CERT: CB-K15/1437 , CB-K15/1188 , CB-K15/0966 , CB-K15/0880 , CB-K15/0854 , CB-K15/0806 , CB-K15/0769 , CB-K15/0763 , CB-K15/0757 , CB-K15/0665 , CB-K15/0648 , CB-K15/0561 , CB-K15/0552 , CB-K15/0207 , DFN-CERT-2016-1004 , DFN-CERT-2015-1514 , DFN-CERT-2015-1252 , DFN-CERT-2015-1017 , DFN-CERT-2015-0926 , DFN-CERT-2015-0900 , DFN-CERT-2015-0842 , DFN-CERT-2015-0809 , DFN-CERT-2015-0803 , DFN-CERT-2015-0794 , DFN-CERT-2015-0697 , DFN-CERT-2015-0677 , DFN-CERT-2015-0583 , DFN-CERT-2015-0579 , DFN-CERT-2015-0212

Other: http://php.net/ChangeLog-5.php
https://bugs.php.net/bug.php?id=69085
http://openwall.com/lists/oss-security/2015/06/01/4

3.1.24) Php Multiple Vulnerabilities - 02 June15 (Windows) 1



Vulnerability	Severity	QoD	Host	Location	Actions
php Multiple Vulnerabilities -02 June15 (Windows)	7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.4
Fixed Version:     5.4.41
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service , bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Impact Level: Application

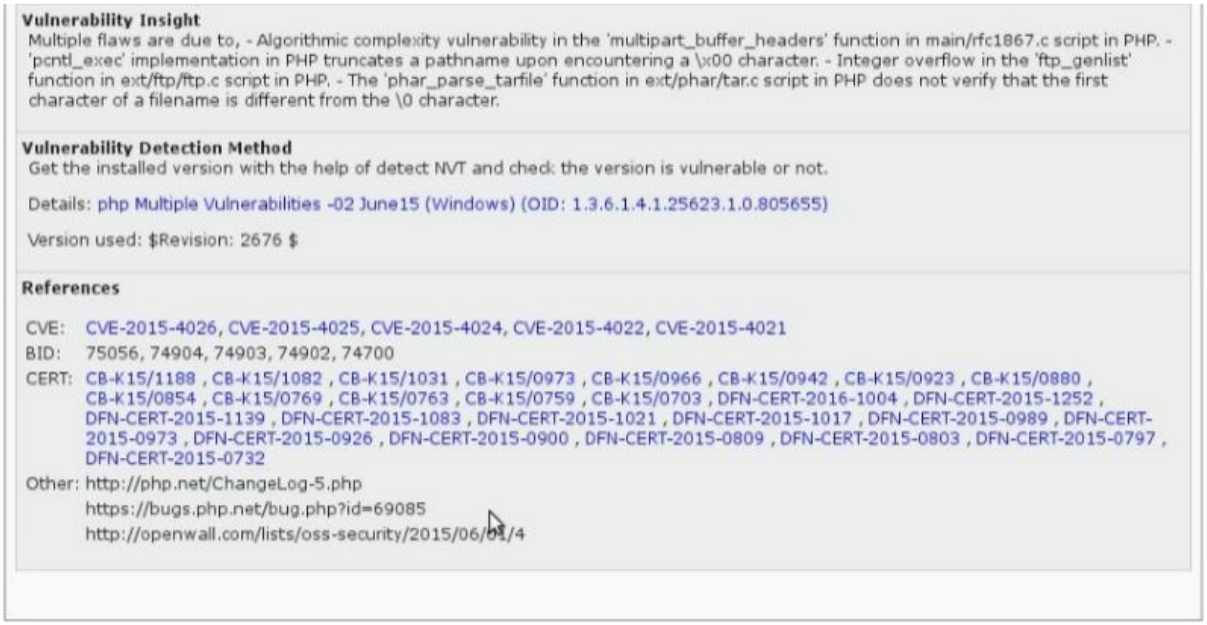
Solution
Solution type: VendorFix

Upgrade to php 5.4.41 or 5.5.25 or 5.6.9 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9

Vulnerability Insight
Multiple flaws are due to, - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character.

3.1.25) Php Multiple Vulnerabilities - 02 June15 (Windows) 2



Vulnerability Insight
Multiple flaws are due to, - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Vulnerabilities -02 June15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.805655)

Version used: $Revision: 2676 $

References

CVE: CVE-2015-4026, CVE-2015-4025, CVE-2015-4024, CVE-2015-4022, CVE-2015-4021

BID: 75056, 74904, 74903, 74902, 74700

CERT: CB-K15/1188 , CB-K15/1082 , CB-K15/1031 , CB-K15/0973 , CB-K15/0966 , CB-K15/0942 , CB-K15/0923 , CB-K15/0880 , CB-K15/0854 , CB-K15/0769 , CB-K15/0763 , CB-K15/0759 , CB-K15/0703 , DFN-CERT-2016-1004 , DFN-CERT-2015-1252 , DFN-CERT-2015-1139 , DFN-CERT-2015-1083 , DFN-CERT-2015-1021 , DFN-CERT-2015-1017 , DFN-CERT-2015-0989 , DFN-CERT-2015-0973 , DFN-CERT-2015-0926 , DFN-CERT-2015-0900 , DFN-CERT-2015-0809 , DFN-CERT-2015-0803 , DFN-CERT-2015-0797 , DFN-CERT-2015-0732

Other: http://php.net/ChangeLog-5.php
https://bugs.php.net/bug.php?id=69085
http://openwall.com/lists/oss-security/2015/06/01/4

3.1.26) Php Multiple Vulnerabilities - 01 June15 (Windows) 1

Vulnerability		Severity	QoD	Host	Location	Actions
php Multiple Vulnerabilities -01 June15 (Windows)		7.5 (High)	80%		8080/tcp	

Summary
This host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.4
Fixed Version:     5.4.39
```

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Impact Level: Application

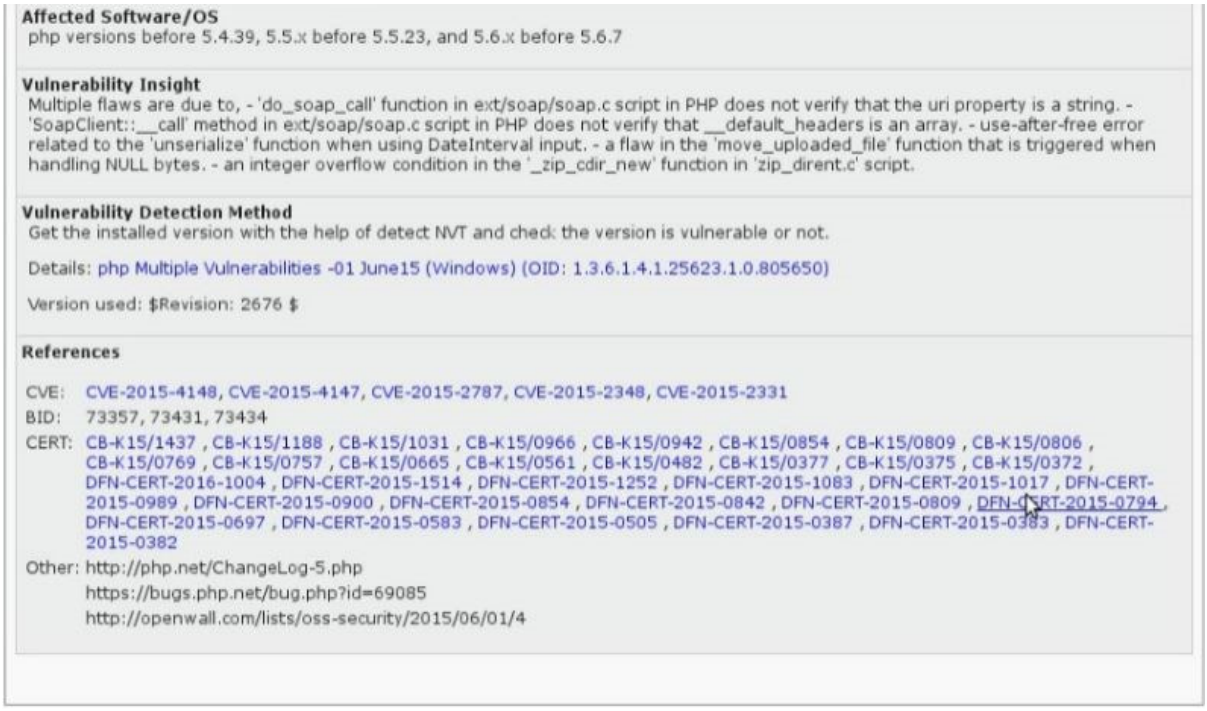
Solution
Solution type: VendorFix

Upgrade to php 5.4.39 or 5.5.23 or 5.6.7 or later. For updates refer to http://www.php.net

Affected Software/OS
php versions before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7

Vulnerability Insight
Multiple flaws are due to, - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script.

3.1.27) Php Multiple Vulnerabilities - 01 June15 (Windows) 2



Affected Software/OS
php versions before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7

Vulnerability Insight
Multiple flaws are due to, - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: php Multiple Vulnerabilities -01 June15 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.805650)

Version used: $Revision: 2676 $

References

CVE: CVE-2015-4148, CVE-2015-4147, CVE-2015-2787, CVE-2015-2348, CVE-2015-2331

BID: 73357, 73431, 73434

CERT: CB-K15/1437 , CB-K15/1188 , CB-K15/1031 , CB-K15/0966 , CB-K15/0942 , CB-K15/0854 , CB-K15/0809 , CB-K15/0806 , CB-K15/0769 , CB-K15/0757 , CB-K15/0665 , CB-K15/0561 , CB-K15/0482 , CB-K15/0377 , CB-K15/0375 , CB-K15/0372 , DFN-CERT-2016-1004 , DFN-CERT-2015-1514 , DFN-CERT-2015-1252 , DFN-CERT-2015-1083 , DFN-CERT-2015-1017 , DFN-CERT-2015-0989 , DFN-CERT-2015-0900 , DFN-CERT-2015-0854 , DFN-CERT-2015-0842 , DFN-CERT-2015-0809 , DFN-CERT-2015-0794 , DFN-CERT-2015-0697 , DFN-CERT-2015-0583 , DFN-CERT-2015-0505 , DFN-CERT-2015-0387 , DFN-CERT-2015-0383 , DFN-CERT-2015-0382

Other: http://php.net/ChangeLog-5.php
https://bugs.php.net/bug.php?id=69085
http://openwall.com/lists/oss-security/2015/06/01/4

3.1.28) Header overflow against HTTP proxy

Vulnerability		Severity	QoD	Host	Location	Actions
Header overflow against HTTP proxy		7.5 (High)	99%		10000/tcp	

Summary
It was possible to kill the HTTP proxy by sending an invalid request with a too long header

A cracker may exploit this vulnerability to make your proxy server crash continually or even execute arbitrary code on your system.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
upgrade your software

Vulnerability Detection Method
Details: Header overflow against HTTP proxy (OID: 1.3.6.1.4.1.25623.1.0.11715)

Version used: $Revision: 3362 $

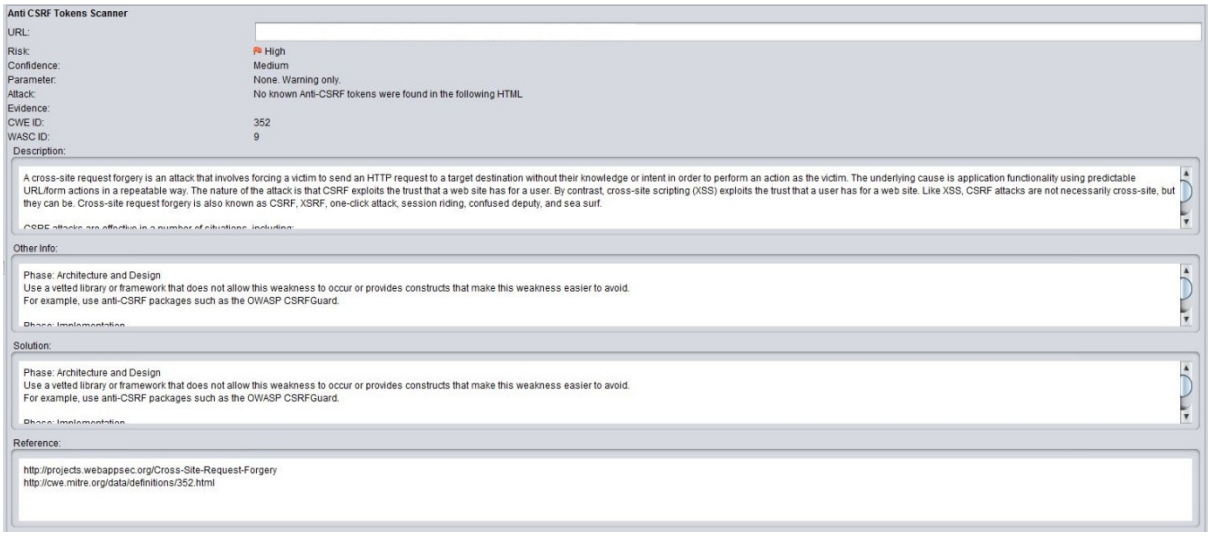
References

CVE: CVE-2002-0133

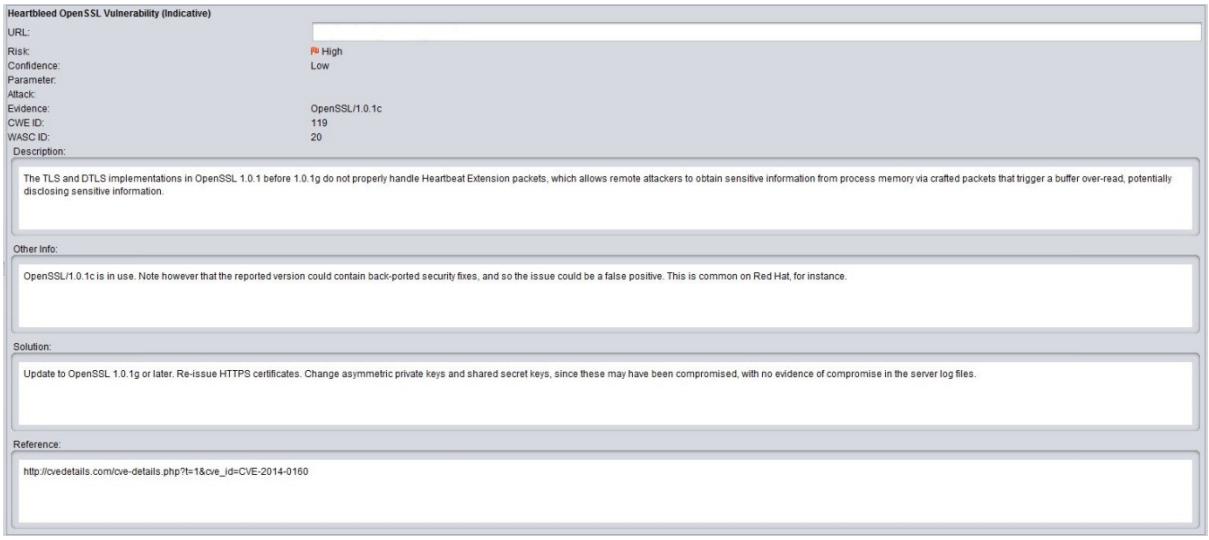
BID: 3904, 3905

3.2) OWASP

3.2.1) Anti-CSRF Tokens Scanner



3.2.2) Heartbleed OpenSSL Vulnerability (Indicative)



3.2.3) Insecure Component – Apache 2.4.2

3.2.4) Insecure Component – Microsoft IIS 7.5

3.2.5) Insecure Component – OpenSSL 1.0.1c

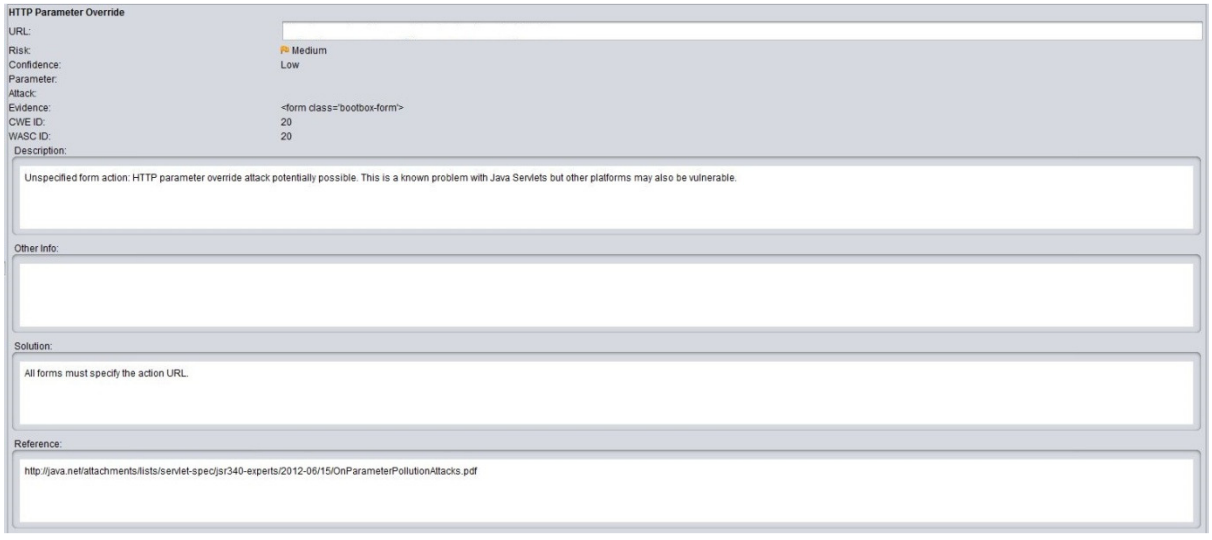
3.2.6) Insecure Component – PHP 5.4.4

3.2.7) Insecure Component – PHP 5.5.9

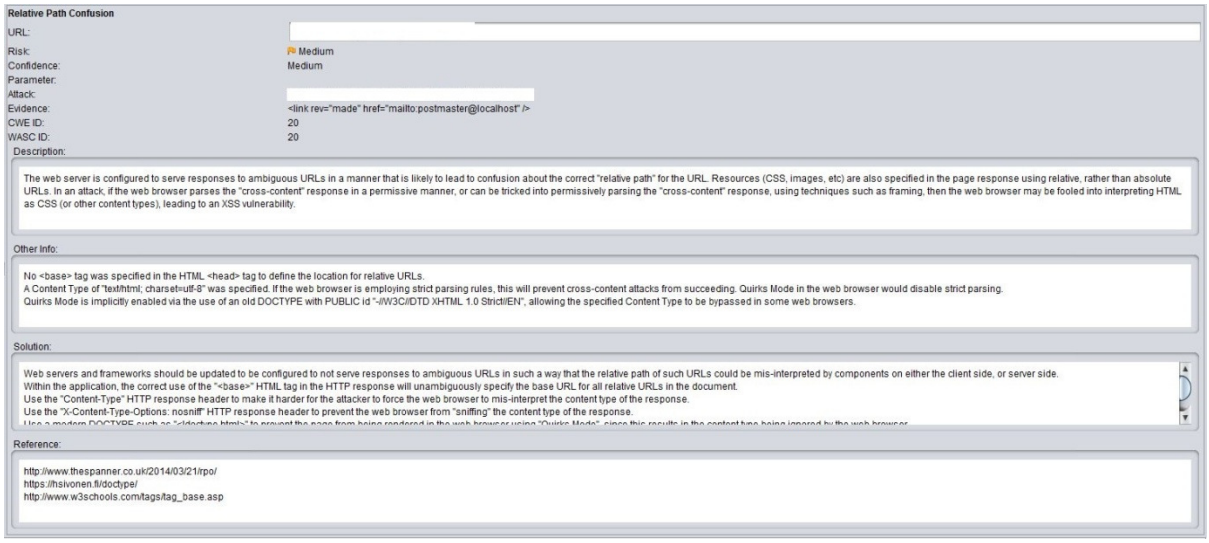
3.2.8) Backup File Disclosure

3.2.9) Directory Browsing

3.2.10) HTTP Parameter Override



3.2.11) Relative Path Confusion



3.2.12) X-Frame-Options Header Not Set

4) Συμπεράσματα

Μετά το πέρας της ολοκλήρωσης της αναζήτησης ευπαθειών στο πληροφοριακό σύστημα του Ιδρύματος και τη καταγραφή τους, έχουμε να κάνουμε τις εξής παρατηρήσεις:

- Πρέπει να γίνεται συνεχόμενος έλεγχος ασφαλείας στα συστήματα.
- Να πραγματοποιείται τακτική αναβάθμιση των λειτουργικών συστημάτων και εφαρμογών που χρησιμοποιούνται.
- Την ενημέρωση των διαφόρων χρηστών για την ορθή χρήση των συστημάτων.
- Συνεχή παρακολούθηση των τεχνικών διείσδυσης σε πληροφοριακά συστήματα και εφαρμογές για την έγκαιρη ενημέρωση και εξάλειψη των ευπαθειών που εμφανίζονται.

Ως συνέχεια της πτυχιακής μας εργασίας θα προτείναμε την αναζήτηση από την αρχή πληροφοριών (Information Gathering), ανάλυση ευπαθειών (Vulnerability Assessment) καθώς και προσπάθεια εκμετάλλευσης ευπαθειών (Exploitation). Σε επόμενο στάδιο είναι επίσης η ανεύρεση των καλύτερων τρόπων για εξάλειψη των ευπαθειών και η καταγραφή τους ανάλογα την ευπάθεια και τον τρόπο εκμετάλλευσής της. Επίσης να γίνει καταγραφή του υπάρχοντος σχεδίου δικτύωσης (Infrastracture) του Ιδρύματος και να διαμορφωθεί σύμφωνα με τα πρότυπα ασφαλείας που ήδη υπάρχουν και εφαρμόζονται.

Συμπέρασμα της πτυχιακής μας εργασίας είναι ότι η ασφάλεια πάντα θα εξελίσσεται μαζί με την ανάπτυξη των πληροφοριακών συστημάτων γι’αυτό απαιτείται συνεχή παρακολούθηση από τους διαχειριστές (administrators).

Ευχαριστούμε τον υπεύθυνο καθηγητή της πτυχιακής μας εργασίας Δρ. Αριστογιάννη Γαρμπή για την ευκαιρία που μας έδωσε, για την ανάλυση του πληροφοριακού συτήματος του Ιδρύματος.

5) Βιβλιογραφία – Πηγές

- «Πολιτική ασφάλειας ΠΣ και ιστορικές αναδρομές»

<https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD_%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD#.CE.91.CE.BA.CE.B5.CF.81.CE.B1.CE.B9.CF.8C.CF.84.CE.B7.CF.84.CE.B1>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 23/08/2014, διαβάστηκε – επεξεργάστηκε: 11/11/2015.

- «Ιοί υπολογιστών»

<https://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 21/04/2015, διαβάστηκε – επεξεργάστηκε: 13/11/2015.

- «Ανάλυση Επικινδυνότητας & Μέτρα Ασφαλείας»

<http://www.icte.uowm.gr/uploads/thesis/dipl_ergasia_am14.pdf>
Λέρα Μαρία, Μελέτη Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων (διπλωματική εργασία), Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών, Πανεπιστήμιο Δυτικής Ελλάδας, Κοζάνη, Ιούνιος 2012. Διαβάστηκε – επεξεργάστηκε: 22/11/2015.

- «Κρυπτογραφία και κρυπταλγόριθμοι»

<https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 13/07/2015, διαβάστηκε – επεξεργάστηκε: 17/11/2015.

- «Πληροφορίες για κρυπτογραφημένα πρωτόκολλα ασφαλείας»

<http://www.utc.edu/faculty/joseph-kizza/docs/guidetonetworksecurity/instructor_support_materials/notes/chapter17.ppt>
Dr. Kizza Joseph Migga, Computers Network Security Protocols, εκδόθηκε: 03/02/2009, διαβάστηκε – επεξεργάστηκε: 17/11/2015.

- «Αναζήτηση στοιχείων Ασφάλειας Συστημάτων Βάσεις Δεδομένων»

<http://eclass.uoa.gr/modules/document/file.php/DI273/%CE%94%CE%B9%CE%B1%CF%86%CE%AC%CE%BD%CE%B5%CE%B9%CE%B5%CF%82%20%CE%B4%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CF%89%CE%BD/06-dbsecurity-bw.pdf>

Εθνικό Καποδιστρικό Πανεπιστήμιο Αθηνών, δημοσιεύτηκε – τροποποιήθηκε: 15/02/2005, διαβάστηκε – επεξεργάστηκε: 04/12/2015.

- «Εύρεση πληροφοριών Σχεδιασμός Ασφαλών ΠΣ & Επίπεδα Προστασίας»

<http://aetos.it.teithe.gr/~vaf/download_files/itsecnotes.pdf>

Δρ. Μπόζιος Ελευθέριος, Εφαρμοσμένη Ασφάλεια Πληροφοριακών Συστημάτων, Τμήμα Πληροφορικής Σ.Τ.ΕΦ., Α.Τ.Ε.Ι. Θεσσαλονίκης, 2004. Διαβάστηκε – επεξεργάστηκε: 23/11/2015.

- «Πληροφορίες για Αρχή Διασφάλισης Απορρίτου των Επικοινωνιών»

<https://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CE%94%CE%B9%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B9%CF%83%CE%B7%CF%82_%CF%84%CE%BF%CF%85_%CE%91%CF%80%CE%BF%CF%81%CF%81%CE%AE%CF%84%CE%BF%CF%85_%CF%84%CF%89%CE%BD_%CE%95%CF%80%CE%B9%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CF%8E%CE%BD>

Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 13/03/2016, διαβάστηκε – επεξεργάστηκε: 24/04/2016.

<http://www.adae.gr/>

Επίσημη ιστοσελίδα, λεπτομέριες για αναφορά και έρευνα. Εκδόθηκε (χ.χ) – τροποποιήθηκε: 2013. Διαβάστηκε – επεξεργάστηκε: 24/04/2016.

- «Λίστα Πέντε Web-Απειλών»

<http://www.naftemporiki.gr/story/807895/pente-web-apeiles-gia-ta-prosopika-dedomena>

Η Ναυτεμπορική – Π. Αθανασιάδης & ΣΙΑ Α.Ε., Άρθρο πέντε web απειλών για τα προσωπικά δεδομένα, εκδόθηκε – υλοποιήθηκε – αναρτήθηκε: 16/05/2014, διαβάστηκε – επεξεργάστηκε: 06/12/2015.

- «SQL Injection, πληροφορίες επιθέσεων και άλλων στατιστικών»

<https://ghostinthelab.wordpress.com/2011/08/24/sql-injection-%CE%B7-%CE%B4%CE%B9%CE%B1%CF%83%CE%B7%CE%BC%CF%8C%CF%84%CE%B5%CF%81%CE%B7-%CE%B5%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7-%CE%B1%CF%80%CE%AD%CE%BD%CE%B1%CE%BD%CF%84%CE%B9-%CF%83%CE%B5-web/>

Ghost in the lab, blog, άρθρο: «SQL Injection: Η διασημότερη επίθεση απέναντι σε web εφαρμογές». Εκδόθηκε – αναρτήθηκε: 24/08/2011, διαβάστηκε – επεξεργάστηκε: 26/02/2016.

<http://openspot.antithesis.gr/archives/33>

Antithesis Group, wordpress openspot: «Πρακτικά θέματα για ανοικτές τεχνολογίες», άρθρο «SQL Injections». Εκδόθηκε – αναρτήθηκε: 15/01/2007, διαβάστηκε – επεξεργάστηκε: 29/02/2016.

<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>
Owasp.org, Official Web-page, άρθρο: «Top ten project». Εκδόθηκε (χ.χ.), τελευταία τροποποίηση: 29/01/2016. Διαβάστηκε – επεξεργάστηκε: 01/03/2016.

- «Cross Site Scripting, πληροφορίες για επιθέσεις, ευπάθειες συστημάτων και παραδείγματα»

<https://el.wikipedia.org/wiki/Cross-site_scripting>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 07/02/2016, διαβάστηκε – επεξεργάστηκε: 03/03/2016.

<https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)>
Owasp.org, Official Web-page, άρθρο: «Cross-site Scripting (XSS)». Εκδόθηκε (χ.χ.) – τροποποιήθηκε: 21/02/2016, διαβάστηκε – επεξεργάστηκε: 08/03/2016.

- «Man in the Middle, πληροφορίες για επιθέσεις»

<https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 02/02/2016, διαβάστηκε – επεξεργάστηκε: 16/03/16.

<https://www.owasp.org/index.php/Man-in-the-middle_attack>
Owasp.org, Official Web-page, άρθρο: «Man-in-the-middle attack». Εκδόθηκε (χ.χ.) – τροποποιήθηκε: 31/08/2015, διαβάστηκε – επεξεργάστηκε: 17/03/16.

- «Πληροφορίες για antivirus & anti-malwares»

<https://en.wikipedia.org/wiki/Antivirus_software>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 07/03/2016, διαβάστηκε – επεξεργάστηκε: 20/03/2016.

- «Αναφορές και πληροφορίες για “Browser Helper Objects”, “Browser hijacking”, “Ransomware”, “Keystroke logging”, “Backdoors, Rootkits”, “Trojan horses”, “Worms”, “LSPs (Layered Service Providers)”, “Fraudtools”, “Adwares”, “Spywares”, “Spamming”, “Scamming (Confidence tricks)”, “Phising”, “Botnet DDoS attacks”»

<https://en.wikipedia.org/wiki/Browser_Helper_Object
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 18/01/2016, διαβάστηκε – επεξεργάστηκε: 20/03/2016.

<https://en.wikipedia.org/wiki/Browser_hijacking>

Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 23/12/2015, διαβάστηκε – επεξεργάστηκε: 20/03/2016.

<https://en.wikipedia.org/wiki/Ransomware>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 17/01/2016, διαβάστηκε – επεξεργάστηκε: 20/03/2016.

<https://en.wikipedia.org/wiki/Keystroke_logging>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 07/12/2015, διαβάστηκε – επεξεργάστηκε: 21/03/2016.

<https://en.wikipedia.org/wiki/Backdoor_(computing)>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 22/02/2016, διαβάστηκε – επεξεργάστηκε: 21/03/2016.

<https://en.wikipedia.org/wiki/Rootkit>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 14/02/2016, διαβάστηκε – επεξεργάστηκε: 23/03/2016.

<https://en.wikipedia.org/wiki/Trojan_horse_(computing)>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 11/03/2016, διαβάστηκε – επεξεργάστηκε: 23/03/2016.

<https://en.wikipedia.org/wiki/Computer_worm>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 21/03/2016, διαβάστηκε – επεξεργάστηκε: 24/03/2016.

<https://en.wikipedia.org/wiki/Layered_Service_Provider>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 03/03/2016, διαβάστηκε – επεξεργάστηκε: 25/03/2016.

<https://en.wikipedia.org/wiki/Rogue_security_software>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 29/02/2016, διαβάστηκε – επεξεργάστηκε: 25/03/2016.

<https://en.wikipedia.org/wiki/Adware>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 24/02/2016, διαβάστηκε – επεξεργάστηκε: 25/03/2016.

<https://en.wikipedia.org/wiki/Spyware>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 17/03/2016, διαβάστηκε – επεξεργάστηκε: 25/03/2016.

<https://en.wikipedia.org/wiki/Spamming>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 24/03/2016, διαβάστηκε – επεξεργάστηκε: 26/03/2016.

<https://en.wikipedia.org/wiki/Confidence_trick>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 05/03/2016, διαβάστηκε – επεξεργάστηκε: 26/03/2016.

<https://en.wikipedia.org/wiki/Phishing>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 19/03/2016, διαβάστηκε – επεξεργάστηκε: 26/03/2016.

<https://en.wikipedia.org/wiki/Botnet>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 26/02/2016, διαβάστηκε – επεξεργάστηκε: 29/03/2016.

<https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 27/03/2016, διαβάστηκε – επεξεργάστηκε: 29/03/2016.

- «Αναφορές και λεπτομέρειες πρωτόκολλων ασφαλείας για "PGP (Pretty Good Privacy)", "S/MIME (Secure/Multipurpose Internet Mail Extension)", "S-HTTP (Secure-Hyper Text Transfer Protocol)", "HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer)", "SET (Secure Electronic Transactions)", "Kerberos" και "SSL (Secure Socket Layers)"»

<https://en.wikipedia.org/wiki/Pretty_Good_Privacy>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 17/02/2016, διαβάστηκε – επεξεργάστηκε: 03/04/2016.

<https://en.wikipedia.org/wiki/S/MIME>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 06/03/2016, διαβάστηκε – επεξεργάστηκε: 03/04/2016.

<https://en.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 19/03/2016, διαβάστηκε – επεξεργάστηκε: 03/04/2016.

<http://searchsoftwarequality.techtarget.com/definition/S-HTTP>
Rouse Margaret, Searchsoftwarequality.techtarget.com, άρθρο: S-HTTP (Secure HTTP), εκδόθηκε – τροποποιήθηκε: Ιανουάριος 2006. Διαβάστηκε – επεξεργάστηκε: 03/04/2016.

<https://el.wikipedia.org/wiki/HTTPS>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 30/03/2016, διαβάστηκε – επεξεργάστηκε: 04/04/2016.

<https://en.wikipedia.org/wiki/Secure_Electronic_Transaction>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 21/03/2016, διαβάστηκε – επεξεργάστηκε: 04/04/2016.

<http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction>
Rouse Margaret, Searchfinancialsecurity.techtarget.com, άρθρο: Secure Electronic Transaction (SET), εκδόθηκε – τροποποιήθηκε: Ιανουάριος 2008. Διαβάστηκε – επεξεργάστηκε: 04/04/2016.

<https://en.wikipedia.org/wiki/Kerberos_(protocol)>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 19/03/2016, διαβάστηκε – επεξεργάστηκε: 04/04/2016.

<https://el.wikipedia.org/wiki/SSL>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 01/05/2016, διαβάστηκε – επεξεργάστηκε: 05/05/2016.

<https://en.wikipedia.org/wiki/Authentication>
Wikipedia, εκδόθηκε (χ.χ.) – τροποποιήθηκε: 09/04/2016, διαβάστηκε – επεξεργάστηκε: 20/05/2016.

- «Χρήσιμες ηλεκτρονικές διευθύνσεις από το Openvas για λεπτομέρειες ευπαθειών.»

1.3) OpenSSL Multiple Vulnerabilities - 02 May 16 (Windows):

<https://www.openssl.org/news/secadv/20160503.txt>
Openssl.org, Official site, άρθρο – αρχείο: "Memory corruption in the ASN.1 encoder (CVE-2016-2108)", εκδόθηκε – τροποποιήθηκε: 03/05/2016, διαβάστηκε – επεξεργάστηκε: 18/07/2016.

1.4) OpenSSL Multiple Vulnerabilities - 01 Mar 16 (Windows):

<https://www.openssl.org/news/secadv/20160301.txt>
Openssl.org, Official site, άρθρο – αρχείο: "Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)", εκδόθηκε – τροποποιήθηκε: 01/03/2016, διαβάστηκε – επεξεργάστηκε: 18/07/2016.

1.5) OpenSSL Multiple Vulnerabilities - 01 May 16 (Windows):

<https://mta.openssl.org/pipermail/openssl-announce/2016-April/000069.html>
Openssl.org, Official site, άρθρο – αρχείο: "Forthcoming OpenSLL releases" εκδόθηκε – τροποποιήθηκε: 28/04/2016, διαβάστηκε – επεξεργάστηκε: 19/07/2016.

1.7) Php Multiple Vulnerabilities - 01 April 16 (Windows):

<https://bugs.php.net/bug.php?id=71587>
Php.net, Official site, άρθρο – αρχείο: "Use-After-Free / Double-Free in WDDX Deserialize", εκδόθηκε: 14/02/2016 – τροποποιήθηκε: 02/03/2016. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

<https://bugs.php.net/bug.php?id=71498>

Php.net, Official site, άρθρο – αρχείο: “Out-of-Bound Read in phar_parse_zipfile()”, εκδόθηκε: 02/02/2016 – τροποποιήθηκε: 03/02/2016. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

<https://secure.php.net/ChangeLog-5.php>
Php.net, Official site, άρθρο – αρχείο: “PHP 5 ChangeLog”, εκδόθηκε (χ.χ.) – τροποποιήθηκε (χ.χ.). Δε χρησιμοποιήθηκε.

1.8) Php ‘phar_fix_filepath’ Function Stack Buffer Overflow Vulnerability

<https://bugs.php.net/bug.php?id=69923>
Php.net, Official site, άρθρο – αρχείο: “Buffer overflow and stack smashing error in phar_fix_filepath”, εκδόθηκε: 24/06/2016 – τροποποιήθηκε: 17/07/2016. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

1.9) Php ‘serialize_function_call’ Function Type Confusion

<http://www.php.net/ChangeLog-5.php>
Php.net, Official site, άρθρο – αρχείο: “PHP 5 ChangeLog”, εκδόθηκε (χ.χ.) – τροποποιήθηκε (χ.χ.). Δε χρησιμοποιήθηκε.

<https://bugs.php.net/bug.php?id=70388>
Php.net, Official site, άρθρο – αρχείο: “SOAP serialize_function_call() type confusion / RCE”, εκδόθηκε: 29/08/2015 – τροποποιήθηκε: 09/09/2015. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

1.10) Php Multiple Vulnerabilities – 01 March16 (Windows)

<https://bugs.php.net/bug.php?id=70068>
Php.net, Official site, άρθρο – αρχείο: “Dangling pointer in the unserialization of ArrayObject items”, εκδόθηκε: 13/07/2015 – τροποποιήθηκε: 09/09/2015. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

<http://www.openwall.com/lists/oss-security/2015/08/19/3>
Openwall.com, Meissner Marcus, απάντηση σε άρθρο: “CVE Request: more php unserializing issues”, εκδόθηκε: 19/08/2015. Διαβάστηκε – επεξεργάστηκε: 19/07/2016.

1.11) OpenSSL Multiple Denial of Service Vulnerabilities – 01 Nov15 (Windows)

<http://www.ubuntu.com/usn/USN-2537-1>
Ubuntu.com, Official site, άρθρο: “Ubuntu Security Notice USN-2537-1, Openssl Vurnerabilities”, εκδόθηκε: 19/03/2015. Διαβάστηκε – επεξεργάστηκε: 20/07/2016.

<https://www.openssl.org/news/secadv/20150319.txt>
Openssl.org, Official site, άρθρο: “OpenSSL 1.0.2 ClientHello sigalgs DoS (CVE-2015-0291)”, εκδόθηκε: 19/03/2015. Διαβάστηκε – επεξεργάστηκε: 20/07/2016.

1.12) php Multiple Remote Code Execution Vulnerabilities July15 (Windows)

<https://bugzilla.redhat.com/show_bug.cgi?id=1194730>

Red Hat Bugzilla, άρθρο: "CVE-2015-0273 php: use after free vulnerability in unserialize() with DateTimeZone", εκδόθηκε: 20/02/2015 – τροποποιήθηκε: 25/11/2015. Διαβάστηκε – επεξεργάστηκε: 20/07/2016.

<http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html>