Γνωστές ευπάθειες από μεγάλες εταιρείες στο χώρο της πληροφορικής έκαναν συστήματα ευάλωτα και τρωτά από εξωτερικές επιθέσεις ή κακόβουλα λογισμικά δημιουργώντας έτσι σοβαρά θέματα ασφαλείας. Μια από τις εταιρείες που είχε ελαττώματα ασφαλείας στα προγράμματα της είναι και η Adobe όπως πολλές άλλες μεγάλες εταιρίες. Παρακάτω θα παρουσιαστούν δύο γνωστά θέματα που προέκυψαν από τέτοια ελαττώματα ασφαλείας κάνοντας τα συστήματα πιο ευπαθή και ευάλωτα. Συγκεκριμένα θα ασχοληθούμε με θέματα ασφαλείας που προέκυψαν το 2015 και το 2016 που είχαν να κάνουν με τον Adobe Flash Player μάλιστα το θέμα ευπάθειας που προέκυψε το 2015 χαρακτηρίστηκε ως κρίσιμης σημασίας. Και τα δύο αυτά τα θέματα αντιμετωπίσθηκαν με επιτυχία σε μεταγενέστερες εκδόσεις – αναβαθμίσεις.

Ευπάθειες Λογισμικού

Αναφορά σε γνωστές ευπάθειες:
Adobe Flash Player
CVE-2015-7645 |
CVE-2016-7855 OpenSSL
CVE-2015-7645 | CVE-2016-7855

a). Η Adobe ενημερώνει σε σχετικό δελτίο με ημερομηνία ανακοίνωσης 14 Οκτωβρίου 2015 με αναγνωριστικό ευπάθειας: APSA15-15 και αριθμό CVE-2015-7645 το οποίο επηρέασε πλατφόρμες: Windows, Macintosh, Linux.
Κρίσιμη ευπάθεια η οποια εντοπίστηκε στον Adobe Flash Player 19.0.0.207 αλλά και νεότερες εκδόσεις συμβατές με λειτουργικά συστήματα: Windows, Macintosh, και Linux. Η κρισιμότητα της συγκεκριμένης ευπάθειάς είναι αρκετά σοβαρή καθώς μία ενδεχόμενη επιτυχής εκμετάλλευσης τις αδυναμίας αυτής θα μπορούσε να τερματίσει τις λειτουργίες του συστήματος και πιθανότατα να οδηγήσει τον επιτιθέμενο στο να πάρει τον έλεγχο του εν λόγω συστήματος που έχει επηρεαστεί.

Εκδόσεις λογισμικού που επηρεάστηκαν:

- Adobe Flash Player 19.0.0.207 και νεότερες εκδόσεις για Windows και Macintosh
- Adobe Flash Player Extended Support Release εκδόσης 18.0.0.252 και νεότερες 18.x εκδόσεις.
- Adobe Flash Player 11.2.202.535 και νεότερες 11.x εκδόσεις για Linux συστήματα.

Στη συνέχεια η Adobe προέτρεψε τους χρήστες να δοκιμάσουν και να ελέγξουν το συστήμα τους με οδηγίες που έχουν να κάνουν με τον εντοπισμό της έκδοσης λογισμικού την οποία τρέχει το σύστημα τους. Στην περίπτωση που οι χρήστες χρησιμοποιούν διαφορετικούς φυλλομετρητές για την περιήγηση στο διαδίκτυο τότε ο έλεγχος θα πρέπει να γίνεται για κάθε ένα φυλλομετρητή ξεχωριστά.

Γενικότερα με τον ορό **Zero Day Exploit:** εννοούμε την επίθεση στον κυβερνοχώρο που συμβαίνει την ίδια μέρα όταν ανακαλύπτεται μια αδυναμία στο λογισμικό. Σε αυτό το σημείο η εκμετάλλευση συμβαίνει πριν μια λύση γίνει διαθέσιμη από το δημιουργό της.
Στη συγκεκριμένη περίπτωση έγινε εκμετάλλευση της ευπάθειας στην «Zero Day» από την ομάδα Pawn Storm η οποία δραστηριοποιείται στον χώρο των κυβερνοεπιθέσεων από το 2007, γνωστή παράλληλα ως : APT28, Sednit, Fancy Bear, Sofacy and Tsar Team. Η ομάδα έβαλε ως στόχο Υπουργεία Εξωτερικών ανά τον κόσμο αλλά και το NATO και το Λευκό Οίκο. Οι επιτιθέμενοι λειτουργούσαν με τη μέθοδο του Phishing εξαπατώντας τους χρήστες μέσω ηλεκτρονικού ταχυδρομείου. Όταν η εκμετάλλευση συνέβαινε με επιτυχία ένα κακόβουλο λογισμικό τύπου

Sednit γινόταν εγκατάσταση στο μηχάνημα του θύματος με αποτέλεσμα να παίρνουν τον έλεγχο των μηχανημάτων προκαλώντας από διαρροές εγγράφων, ζημιές ή και τον απόλυτο έλεγχο.
Ο εντοπισμός έγινε από τον Peter Pi της εταιρείας Trend Micro που ανέφερε το CVE-2015-7645 και συνεργάστηκε με την εταιρεία στο να βοηθήσει για την προστασία των πελατών της. Ενώ παράλληλα η Natalie Sivanovich της Google προσέφερε βοήθεια στην ανάλυση των θεμάτων προς επίλυση.

Το πρόβλημα διορθώθηκε αμέσως την επόμενη μέρα - 16 Οκτωβρίου 2015. CVE-2015-7645 | **CVE-2016-7855**

Στις 26 Οκτωβρίου το 2016 ένα security update to Adobe flash player παρουσίασε μια ακόμη μεγάλη ευπάθεια με αναγνωριστικό ευπάθειας : APSB16-36 και προτεραιότητα 1. Οι πλατφόρμες που επηρεάστηκαν ηταν : Windows, Machintosh, Linux και Chrome OS.
Χαρακτηρίστηκε επίσης ως κρίσιμη καθώς Ο επιτιθέμενος θα μπορούσε να πάρει τον έλεγχο των συστημάτων των οποίων είχε πιθανόν αποκτήσει πρόσβαση.

Εκδόσεις λογισμικού που επηρεάστηκαν:

Προϊόν	Επηρεασμένες έκδοσες	Πλατφόρμες
Adobe Flash Player Desktop Runtime	23.0.0.185 και νεότερες	Windows, Macintosh, Linux και Chrome OS
Adobe Flash Player για Google Chrome	23.0.0.185 και νεότερες	Windows 10 και 8,1
Adobe Flash Player για Microsoft Edge και Internet Explorer 11	11.2.202.637 και νεότερες	
Adobe Flash Player για Linux	23.0.0.185 και νεότερες	Windows και Macintosh

23.0.0.185 και νεότερες Windows,

Στη συνέχεια η Adobe δίνει οδηγίες για τον εντοπισμό και επαλήθευσης τις εκδόσης της οποίας κατέχουν οι χρήστες. Σε περίπτωση που οι χρήστες χρησιμοποιούν πολλούς φυλλομετρητές τότε ο έλεγχος θα πρέπει να γίνει για κάθε έναν φυλλομετρητή που έχει γίνει εγκατάσταση στο σύστημα.

Λύση:

Η Adobe κατηγοριοποιεί τις αναβαθμίσεις και προτρέπει τους χρήστες να εγκαταστήσουν την νεότερη έκδοση.

Προϊόν	Αναβαθμισμένη έκδοση	Πλατφόρμα	Βαθμός προτεραιότητας	Διαθεσιμότητα
Adobe Flash Player Desktop Runtime				
Adobe Flash Player για Google Chrome				
Adobe Flash Player για Microsoft Edge και Internet Explorer 11				

23.0.0.205 Windows και Macintosh	Linux και Chrome OS	Distribution 1 Google Chrome Releases
	23.0.0.205 Windows 10 και 8.1	
23.0.0.205 Windows Macintosh	1 Flash Player Download Center Flash Player	1 Microsoft Security Advisory
	Player για Linux 11.2.202.643 Linux 3 Flash player Download Centre	
Adobe Flash		

Η ευπάθεια, CVE-2016-7855, αποκαλύφθηκε από τους Neel Mehta και Billy Leonard της ομάδας ανάλυσης απειλών της Google. Η ερευνητές επιβεβαίωσαν την εκμετάλλευση της ευπάθειας σε κάποιες στοχοθετημένες επιθέσεις εναντίον χρηστών που χρησιμοποιούσαν windows 7, 8.1 και 10.

CVE-2015-7645 | CVE-2016-7855

β). Σύμφωνα με τον οργανισμό : CVE
Στη διεύθυνση : http://cve.mitre.org/

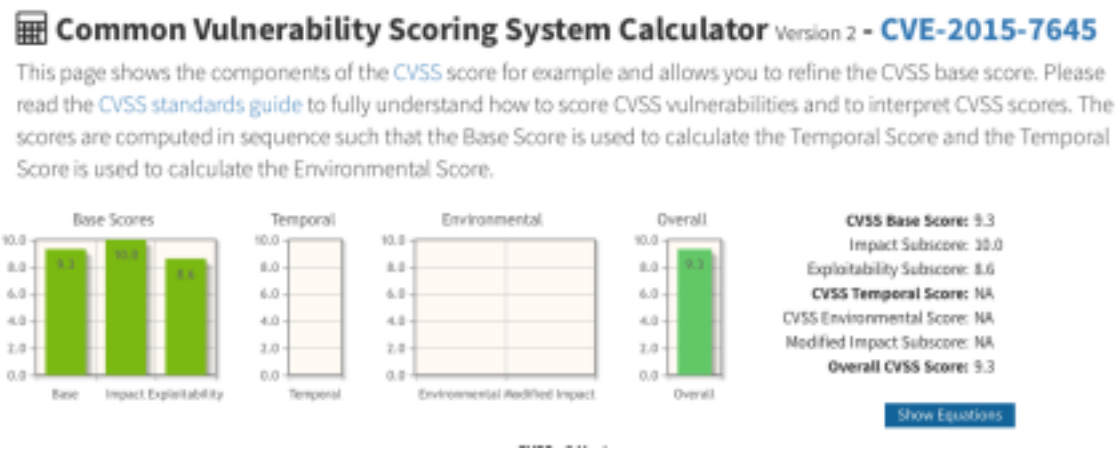
Το Adobe flash player 18.X έως 18.0.0.252 και 19.X έως 19.0.0.207 σε Windows και Mac OS και 11.X έως 11.2.202.535 σε Linux περιβάλλον παρουσίασε γνώστη ευπάθεια κάνοντας δυνατή σε απομακρυσμένους εισβολείς να εκτελέσουν αυθαίρετο κώδικα μέσω ενός crafted αρχείου SWF όπως συνέβη τον Οκτώβριο το 2015.

CVE-2015-7645 **| CVE-2016-7855**

Η ευπάθεια χρήσης που παρουσιάστηκε στον Adobe Flash Player πριν από το 23.0.0.205 στα Windows και Mac OS αλλά και πριν από το 11.2.202.643 στο Linux έκανε δυνατή την πρόσβαση σε απομακρυσμένους εισβολείς οι οποίοι μπορούσανε να εκτελέσουν αυθαίρετους κώδικες μέσω απροσδιόριστων διανυσμάτων. Η συγκεκριμένη ευπάθεια εκμεταλλεύτηκε τον Οκτώβριο του 2016.
Οι ευπάθειες που είναι καταχωρημένες στη συγκεκριμένη βάση δεδομένων της ιστοσελίδας σχετικές με το Adobe flash player είναι 17 στο σύνολο. Στην ιστοσελίδα : cvedetails.com υπάρχουν καταγεγραμμένες 2533 ευπάθειες της Adobe από το 1999 μέχρι το 2018. Οι περισσότερές ευπάθειες σημειώθηκαν το 2016 και ήταν 548 στο σύνολο. Το προϊόν adobe flash player σημειώνει τις περισσότερες ευπάθειες και είναι 1048 στο σύνολο.

CVE-2015-7645 | CVE-2016-7855

γ). Σύμφωνα με την ιστοσελίδα: https://nvd.nist.gov
Η σοβαρότητα της ευπάθειάς αυτής είναι 9,3

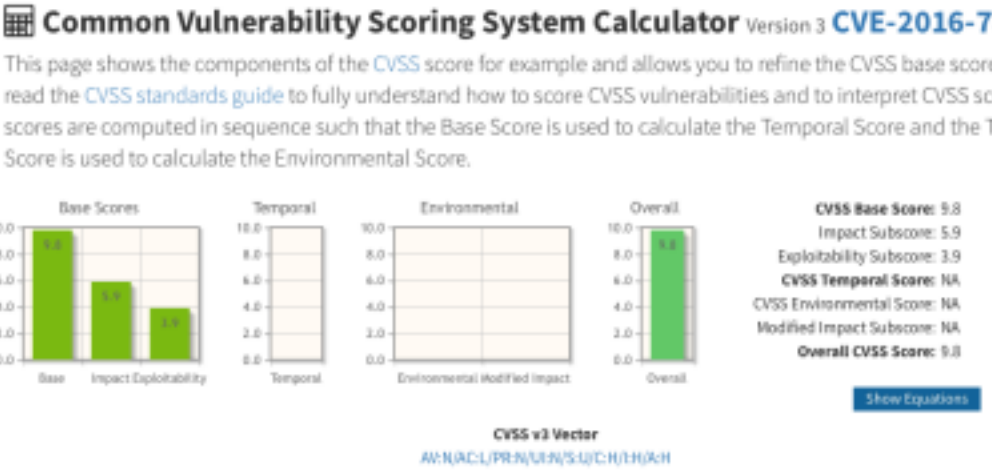


Εικόνα 1.1

Στο γράφημα παρουσιάζεται ο αναλυτικός τρόπος από το οποίο προκύπτουν μέσω των μετρικών που εφαρμόζονται η βαθμολογία της σοβαρότητας (severity)

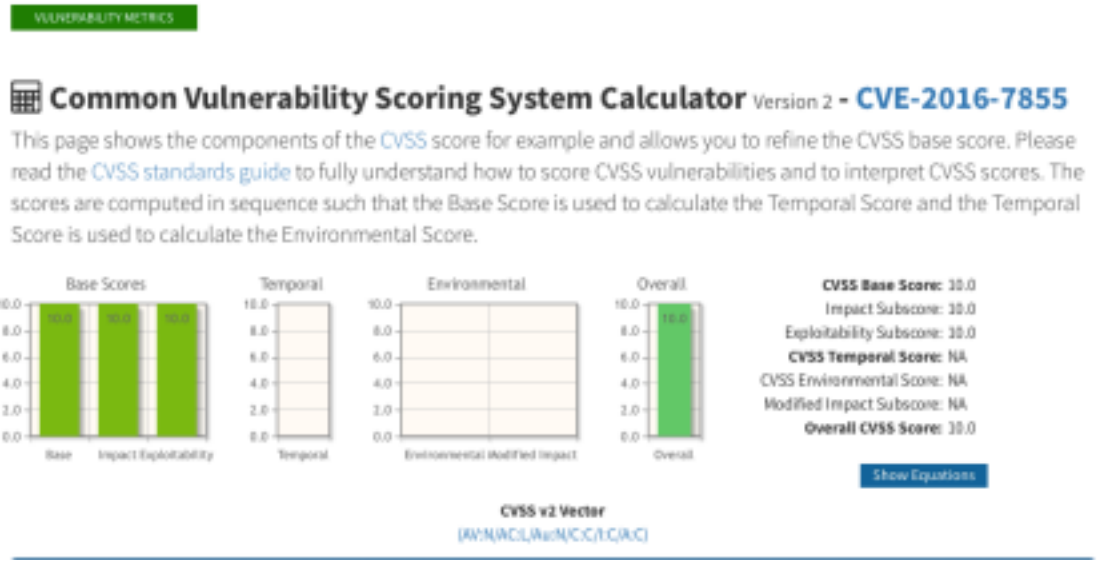
CVE-2015-7645 | CVE-2016-7855

Η σοβαρότητα της ευπάθειας βαθμολογείται με 9,8 στα Windows.



Εικόνα 1.2

Ενώ στα λειτουργικά συστήματα Linux με 10.



Εικονα 1.3

CVE-2015-7645 | CVE-2016-7855

δ).

Στην ιστοσελίδα security focus.com παρέχονται λεπτομερείς πληροφορίες σχετικά με την ευπάθεια αυτή μάλιστα και κάποιες πληροφορίες με τις πιο σταθερές εκδόσεις, που δεν έχουν δηλαδή ευπάθειες.

Not Vulnerable: Adobe Flash Player 19.0.0.226
Adobe Flash Player 18.0.0.255
Adobe Flash Player 11.2.202.540

CVE-2015-7645 **| CVE-2016-7855**

Αντίστοιχα και για την ευπάθεια αυτή παρέχονται λεπτομερείς πληροφορίες καθώς και δύο εκδόσεις που δεν παρουσιάζουν ευπάθειες.

Not Vulnerable: Adobe Flash Player 23.0.0.205
Adobe Flash Player 11.2.202.643

ε).

Γνωστές ευπάθειες του OpenSSL

I. Έχουν εντοπιστεί 278 ευπάθειες από το 2000 μέχρι και 2018.
Πρώτη καταχώρηση : **CVE-2000-1254**
Τελευταία: CVE-2018-0739

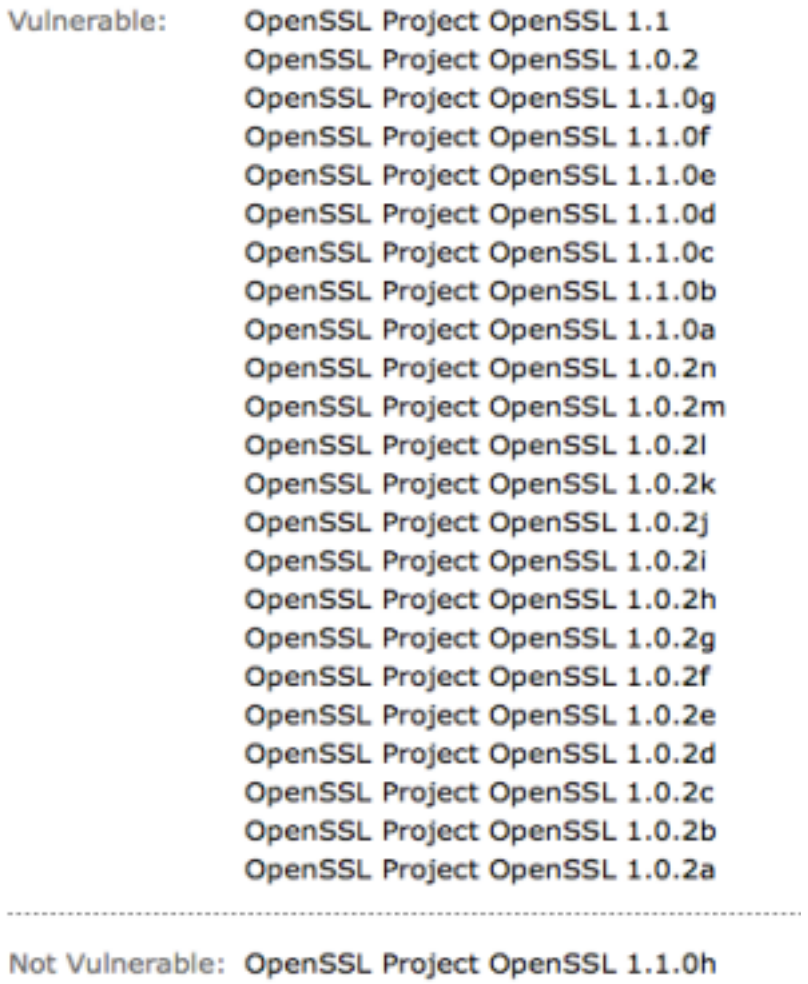
II. Δεν παρέχονται πληροφορίες σχετικά με την σοβαρότητα της ευπάθειας για τη συγκεκριμένη πρόσφατη καταχώρηση CVE-2018- 0739**.**

Vuln ID	Summary	CVSS Severity
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n). **Published:** March 27, 2018; 05:29:00 PM -04:00	(not available)

Εικόνα 2.1

III. Για την ευπάθεια: CVE-2018-0739 η ιστοσελίδα: securityfocus.com
Δίνει τις εξής πληροφορίες:
Αναγνωριστικό bug: 103518
Κλάση: αποτυχία διαχείρισης Exceptional Conditions.
Αφορούσε τους χρήστες που χειριζόντουσαν το σύστημα απομακρυσμένα και όχι εκείνους που χειριζόντουσαν σε τοπικό μηχάνημα. Δημοσιεύτηκε 27 Μαρτίου 2018 και η αναβάθμιση έγινε την ίδια μέρα. Η ευπάθεια εντοπίστηκε από τον Matt Casswell.

Παρατίθεται μια λίστα με τις ευπαθείς εκδόσεις:



Εικόνα 2.2

Από την εικόνα βλέπουμε και τη μία και μοναδική έκδοση του OpenSSL OpenSSL 1.1.0h η οποία δεν ανήκει στις ευπαθείς εκδόσεις και είναι ασφαλής για χρήση.

Πηγές πληροφοριών που χρησιμοποιήθηκαν :
https://blog.trendmicro.com/trendlabs-security-intelligence/latest flash-exploit-used-in-pawn-storm-circumvents-mitigation techniques/

‘Αμπελ Μπάσα, Αθήνα 4 Απριλίου 2018