ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Εργασία Μαθήματος ***Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση *<<αριθμός άσκησης>>*	***<<Τίτλος άσκησης>>***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	29-10-2018

Εκφώνηση της άσκησης

Με βάση το παρακάτω παράδειγμα, καλείστε να πραγματοποιήσετε μία καταγραφή των υπηρεσιών και των αγαθών του ΠΣ το οποίο θα χρησιμοποιήσετε για την εργασία του μαθήματος, καθώς και μία αρχική μελέτη ασφάλειας του συστήματος.

(1) Καταγραφή του υπό μελέτη συστήματος. Να πραγματοποιήσετε για το δικό σας ΠΣ μία αρχική καταγραφή των υπηρεσιών και της αρχιτεκτονικής του συστήματος. Να περιγράψετε τουλάχιστον 3 υπηρεσίες του ΠΣ. (1-2 σελίδες με βάση το παραπάνω ενδεικτικό παράδειγμα και ανάλογα με το δικό σας Πληροφοριακό Σύστημα)

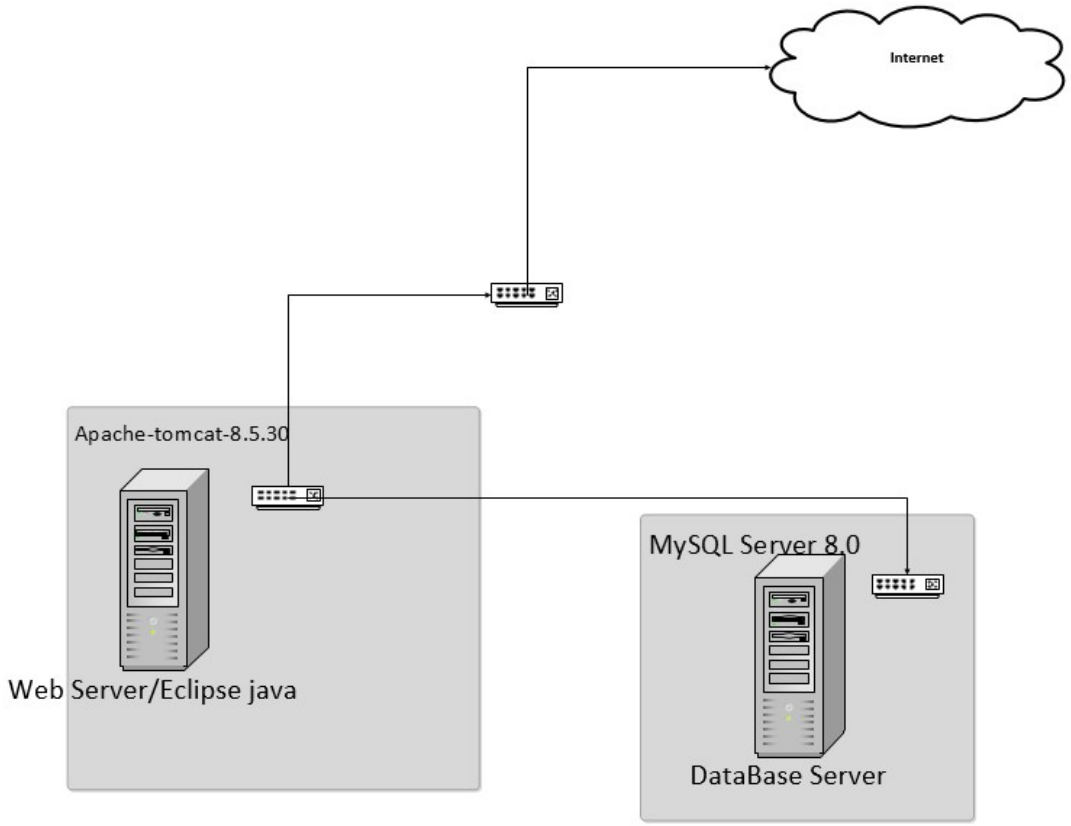
Ηλεκρτονικό Κατάστημα με Κινητά Τηλέφωνα

1)**Εμφανιση Προιόντων:**Παρέχει την δυνατότητα στούς χρήστες (εγγεγραμένους ή οχι) να βλέπουν τα προιόντα.

2)Εγγραφή Χρηστών:Οι χρήστες εγγράφονται για τις υπηρεσίες του ηλεκτρονικού καταστήματος μεσω web form παρέχοντας στοιχεία Όνομα,Επίθετο,Αριθμός τηλέφώνου,Διεύθυνση Κατοικίας.

3)Ηλεκτρονική Παραγγελία: Οι εγγεγραμμένοι χρήστες έχουν την δυνατότητα να πραγματοποιήσουν ηλεκτρονικές παραγγελίες .Ο διαχειριστής θα εγρίνει την παραγγελία του χρήστη με μια ηλεκτρονική σφραγιδα την οποια και θα δείχνει στον διανομέα.

Αρχιτεκτονική Δικτύου δίδεται στο παρακάτω σχήμα.



Οι τεχνολογίες πάνω στις οποίες έχει υλοποιηθεί η παραπάνω υπηρεσία είναι ακόλουθες:

-Λειτουργικο Συστημα: Windows 10 Version10.0.17134 Build 17134

-Εξυπηρετητής Ιστού: Apache-tomcat-8.5.30

-Εξυπηρετητής εφαρμογής: java 8(64 bit)

-Εξυπηρετητής βάσης δεδομένων:MySql Server 8.0

-Πλαίσιο υλοποίησης (framework): Eclipse-inst-win64

(2) Δημιουργία μοντέλου αγαθών (asset model).). Για κάθε υπολογιστικό σύστημα που αποτελεί μέρος του ΠΣ που έχετε περιγράψει στο προηγούμενο βήμα, να μοντελοποιήσετε αναλυτικά όλα τα αγαθά του υπολογιστικού συστήματος (H/W, S/W, Network, Data). Να καταγράψτε το μοντέλο αγαθών για 3 υπολογιστικά συστήματα. Για την μοντελοποίηση μπορείτε να χρησιμοποιήσετε τον παρακάτω πίνακα για την μοντελοποίηση των αγαθών κάθε Υπολογιστικού Συστήματος.

Όνομα Υπολογιστικού Συστήματος:

HW	Server (Μοντέλο,Χαρακτηριστικά)	Apache Tomcat 8.5 MySql Server 8.0
HW	Τοποθεσία(κτίριο,Δωμάτιο)	Γαλατσι,Χριστιανουπόλεως 61
SW	Λειτουργικό Σύστημα(Πυρήνας,Έκδοση)	Windows-Version 10.0.17134 Build 17134
SW	Λογισμικό Εφαρμογών	Java 6 Eclipse jee-Oxygen
Network	Περιοχή Δυκτίου	
Network	Σημείο Σύνδεσης	
Data	Δεδομένα Διαμόρφωσης	Χρήστες,Διαχειριστές
Data	Δεδομένα λειτουργίας Συσκευής	Κινήτα τηλέφωνα

(3) Αντιστοίχηση υπηρεσιών και υπολογιστικών συστημάτων. Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αντιστοιχίσετε τα υπολογιστικά συστήματα που χρησιμοποιούνται για την παροχή της υπηρεσίας (από αυτά που περιγράψατε στο βήμα 2). Είναι πιθανό ένα υπολογιστικό σύστημα να χρησιμοποιείται για την παροχή περισσότερων από μία υπηρεσιών.

Εμφανιση Προιόντων ->SWΛογισμικό Εφαρμογών

Εγγραφή Χρηστών-> HW Server

Ηλεκτρονική Παραγγελία->Network Σημείο Σύνδεσης

(4) Αποτίμηση συνεπειών ή επιπτώσεων ασφάλειας (impact assessment). Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αποτιμήσετε τις πιθανές συνέπειες ασφάλειας (security impact) από την πιθανή παραβίαση της ασφάλειας των αγαθών που συμμετέχουν στην κάθε υπηρεσία, ως εξής:

- Συνέπειες μη διαθεσιμότητας της υπηρεσίας (unavailability / loss of Availability).
- Συνέπειες αποκάλυψης των δεδομένων που διαχειρίζεται η υπηρεσία (disclosure / loss of Confidentiality).
- Συνέπειες τροποποίησης των δεδομένων που διαχειρίζεται η υπηρεσία (modification / loss of Integrity).

Ο Τύπος Συνέπειας θα έχει μία ή περισσότερες από τις παρακάτω επιλογές:

- Άμεσες οικονομικές απώλειες
- Παρεμπόδιση λειτουργιών
- Δυσφήμιση
- Νομικές Κυρώσεις

Ο Βαθμός Συνέπειας θα έχει μία από τις παρακάτω τιμές:

1. Χαμηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος μέχρι €100/περιστατικό.

2. Μέτρια: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος από €101 μέχρι €1.000/περιστατικό.

3. Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €1.001 μέχρι €10.000/περιστατικό.

4. Πολύ Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €10.000/περιστατικό.

Η αποτίμηση συνεπειών θα γίνει, για κάθε υπηρεσία με τη βοήθεια του παρακάτω πίνακα:

'Ονομα Υπηρεσίας	**Εμφανιση Προιόντων**

	Τύπος Συνέπειας	**Βαθμός Συνέπειας**	**Συντομη Αιτιολόγηση**
Συνεπειες για:			
(1)Μη Διαθεσιμοτητα	Δυσφήμιση	Μετρια	Η ζημια θα προκυψει για μερικές ώρες
(2)Αποκάλυψη Δεδομένων	Καμία	Κανένας	Τα στοιχεία είναι δημόσια
(3)Τροποποίηση Δεδομένων	Αμεσες Οικονομικές Απώλειες	Υψηλή	Αλαγή στο ποσό αγοράς προιόντος

‘Ονομα Υπηρεσίας	Εγγραφή Χρηστών

	Τύπος Συνέπειας	Βαθμός Συνέπειας	Συντομη Αιτιολόγηση
Συνεπειες για:			
(1)Μη Διαθεσιμοτητα	Αμεσες Οικονομικές Απώλιες	Υψηλή	Οι χρηστες δεν θα είναι σε θέση να αγοράζουν προίοντα
(2)Αποκάλυψη Δεδομένων	Νομικές Κυρώσεις	Πολύ Υψηλή	Πρόστιμο απο όλους τους χρήστες
(3)Τροποποίηση Δεδομένων	Παρεμπόδιση Λειτουργιών	Υψηλή	Δεν πραγματοποιούνται παραγγελιές προιόντων

‘Ονομα Υπηρεσίας	Ηλεκτρονική Παραγγελία

	Τύπος Συνέπειας	Βαθμός Συνέπειας	Συντομη Αιτιολόγηση
Συνεπειες για:			
(1)Μη Διαθεσιμοτητα	Δυσφήμιση	Υψηλή	Δεν πραγματοποιείται Πώληση προιόντων
(2)Αποκάλυψη Δεδομένων	Νομικές Κυρώσεις	Πολύ Υψηλή	Προστιμο απο τους χρήστες που πραγματοποιησαν παραγγελίες
(3)Τροποποίηση Δεδομένων	Αμεσες Οικονομικές Απώλιες	Υψηλή	Δεν παραδίδονται τα προιόντα στους χρήστες

(5)Αποτίμηση απειλών(threat assessment). Να αξιολογήσετε τις παρακάτω απειλές για κάθε ένα από τα 3 υπολογιστικά συστήματα που καταγράψατε στο βήμα 2:

- **Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access).**
- **Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware).**
- **Παραποίηση ιστοσελίδας (Web Defacement).**
- **Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection).**

• Άρνηση υπηρεσίες (Denial of Service).

Η αποτίμηση κάθε απειλής για κάθε ένα από τα 3 υπολογιστικά συστήματα που μελετάτε, θα γίνει με βάση την κλίμακα:

0. Δεν εφαρμόζεται (not applicable): Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.

1. Χαμηλή πιθανότητα (Low likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%. 3

2. Μέτρια πιθανότητα (Medium likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 30%.

3. Υψηλή πιθανότητα (High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.

4. Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

1)Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access).

Χαμηλή πιθανότητα (Low likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%. 3

2)Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware).

Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

3)Παραποίηση ιστοσελίδας (Web Defacement).

Υψηλή πιθανότητα (High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.

4)Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection).

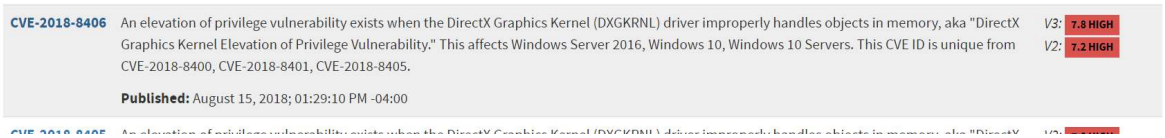
0. Δεν εφαρμόζεται (not applicable): Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.

5) • Άρνηση υπηρεσίες (Denial of Service).

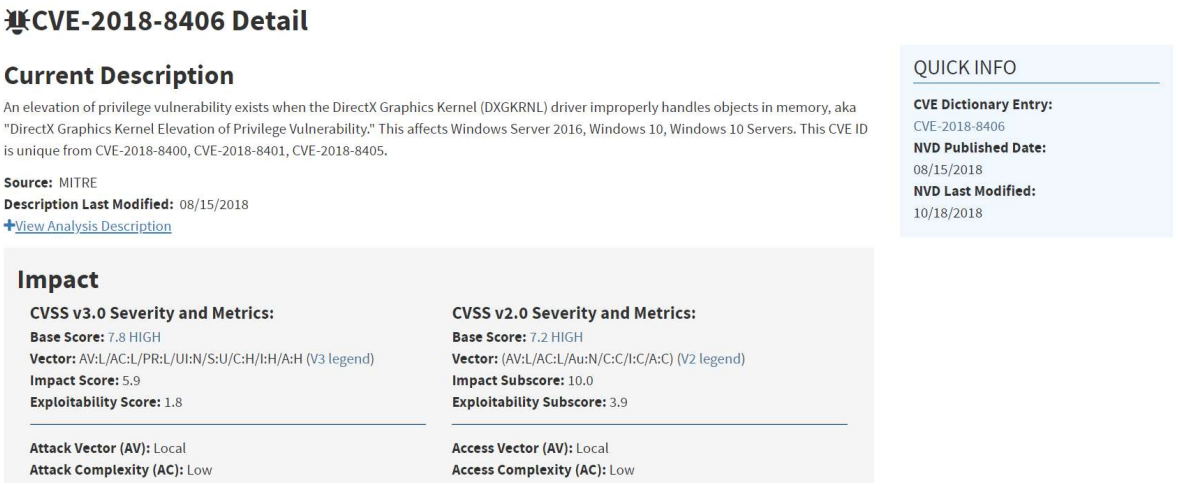
4. Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

(6)Αποτίμηση αδυναμιών (vul).nerabil).ity assessment). Να γίνει αποτίμηση αδυναμιών για όλα τα αγαθά λογισμικού των τριών υπό μελέτη υπολογιστικών συστημάτων (Λειτουργικό Σύστημα, λογισμικό εφαρμογών). Να χρησιμοποιήσετε διαθέσιμες βάσεις αδυναμιών π.χ. τη βάση αδυναμιών ασφάλειας του NIST (http :// nvd. nist. gov /). Στην έρευνά σας θα πρέπει να συγκεντρώσετε και να περιγράψετε τις βασικότερες αδυναμίες ασφάλειας που υπάρχουν για τις συγκεκριμένες εκδόσεις λογισμικού που περιλαμβάνονται στα υπό μελέτη υπολογιστικά συστήματα.

Λειτουργικο Συστημα: Windows 10 Version 10.0.17134 Build 17134



CVE-2018-8406	An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objects in memory, aka "DirectX Graphics Kernel Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8400, CVE-2018-8401, CVE-2018-8405. **Published:** August 15, 2018; 01:29:10 PM -04:00	*V3:* 7.8 HIGH *V2:* 7.2 HIGH



CVE-2018-8406 Detail

Current Description

An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objects in memory, aka "DirectX Graphics Kernel Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8400, CVE-2018-8401, CVE-2018-8405.

Source: MITRE
Description Last Modified: 08/15/2018
View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2018-8406
NVD Published Date:
08/15/2018
NVD Last Modified:
10/18/2018

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 7.8 HIGH
Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 1.8

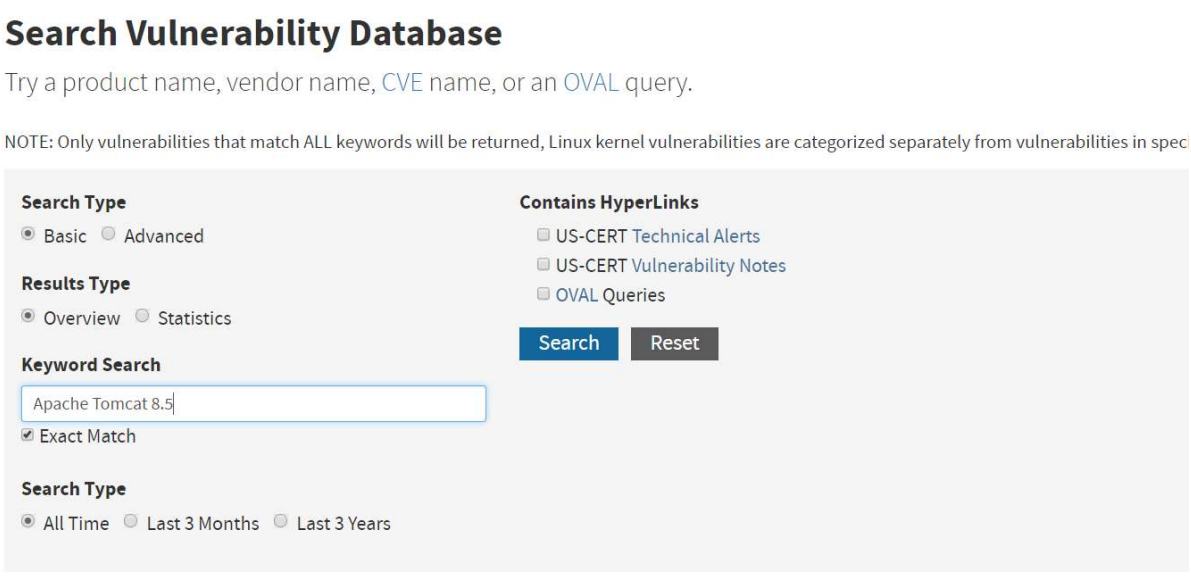
Attack Vector (AV): Local
Attack Complexity (AC): Low

CVSS v2.0 Severity and Metrics:
Base Score: 7.2 HIGH
Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.9

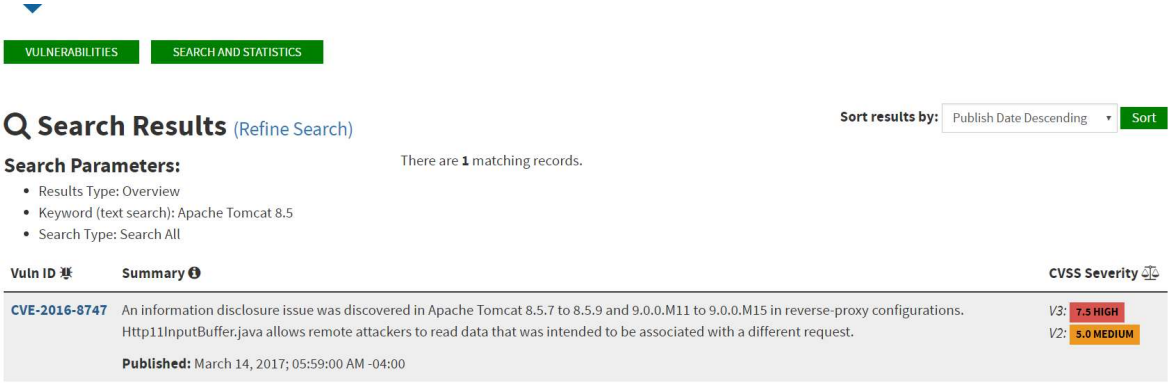
Access Vector (AV): Local
Access Complexity (AC): Low

https://nvd.nist.gov/vuln/detail/CVE-2018-8406

Εξυπηρετητής Ιστου Apache-tomcat-8.5.30



Ψαχνω για αδυναμίες στον apache tomcat 8.5



VULNERABILITIES SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

There are 1 matching records.

Search Parameters:

- Results Type: Overview
- Keyword (text search): Apache Tomcat 8.5
- Search Type: Search All

Vuln ID	Summary	CVSS Severity
CVE-2016-8747	An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-proxy configurations. Http11InputBuffer.java allows remote attackers to read data that was intended to be associated with a different request. **Published:** March 14, 2017; 05:59:00 AM -04:00	V3: 7.5 HIGH V2: 5.0 MEDIUM

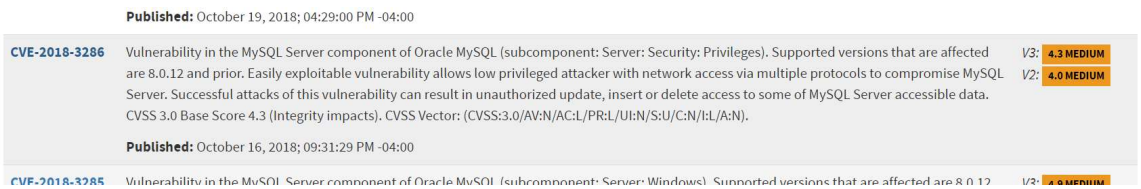
Current Description

An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-proxy configurations. Http11InputBuffer.java allows remote attackers to read data that was intended to be associated with a different request.

Εξηπηρετητης Εφαρμογής:java 8(64 bit)

Δεν υπάρχουν διαθέσιμες αδυναμίες

-Εξυπηρετητής βάσης δεδομένων:MySql Server 8.0



	Published: October 19, 2018; 04:29:00 PM -04:00	
CVE-2018-3286	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **Published:** October 16, 2018; 09:31:29 PM -04:00	V3: 4.3 MEDIUM V2: 4.0 MEDIUM
CVE-2018-3285	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Windows). Supported versions that are affected are 8.0.12	V3:

the information provided.

Current Description

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

Source: MITRE
Description Last Modified: 10/16/2018
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 4.3 MEDIUM
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N (V3 legend)
Impact Score: 1.4
Exploitability Score: 2.8

CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:N/I:P/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

https://nvd.nist.gov/vuln/detail/CVE-2018-3286

Current Description

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible

data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).