NETSPARKER

Found Vulnerabilities

File View Reporting Tools Help

Start New Scan | Start Incremental Scan | Pause | Skip Current Phase | Import Links | Start Proxy

Site Map

- Out-of-date Version (jQu
- Out-of-date Version (Tomcat)
- Version Disclosure (Tomcat)
- search.html
- cgi-bin
- Forbidden Resource
- server-status
- Apache Server-Status Detected
- online-banking.html
- feedback.html
- [Possible] Cross-site Request For
- index.html
- login.html
- ?login_error
- Password Transmitted over HTTP
- [Possible] Cross-site Request For
- HTTP Strict Transport Security (HSTS)
- faq.html
- help.html
- ?topic
- Cross-site Scripting via Remc
- [Possible] Source Code Disclo

Vulnerability | Browser View | HTTP Request / Response

Controlled Scan | Retest | Send to Request Builder | Generate WAF Rules | Execute SQL Commands | Get Shell | LFI Exploitation | Generate Exploit | Short Names

Out-of-date Version (Tomcat)

CRITICAL

CERTAINTY	
URL	http://zero.webappsecurity.com/resources/
IDENTIFIED VERSION	7.0.70 (contains 4 critical and 45 other vulnerabilities)
LATEST VERSION	10.0.11
VULNERABILITY DATABASE	Result is based on 10-09-2021 vulnerability database content.

CLASSIFICATION

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
CAPEC	310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of Tomcat.

REMEDY

Please upgrade your installation of Tomcat to the latest stable version.

REMEDY REFERENCES

Vulnerability | Scan | Request Builder

Dashboard

Crawling & Attacking (2/3)...

86%

8457 / 9829

Scan Information

Current Speed:	9.4 req/sec
Average Speed:	14.4 req/sec
Total Requests:	11846
Failed Requests:	3
HEAD Requests:	557
Elapsed Time:	00:13:44

Issues (36)

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected
- [Possible] Source Code Disclosure (PHP)
- Insecure Transportation Security Protocol Supported (TLS 1.0)

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Issues (36) | Encoder | Logs (10)

Auto save finished successfully - 12-09-2021 20:30:26

Successfully updated vulnerability database to v2021.09.10.2030

Proxy: System

Type here to search

29°C ENG 20:38 12-09-2021

File View Reporting Tools Help

Start New Scan | Start Incremental Scan | Pause | Skip Current Phase | Import Links | Start Proxy

Site Map

- Out-of-date Version (jQu
- Out-of-date Version (Tomcat)
- Version Disclosure (Tomcat)
- search.html
- cgi-bin
- Forbidden Resource
- server-status
- Apache Server-Status Detected
- online-banking.html
- feedback.html
- [Possible] Cross-site Request For
- index.html
- login.html
- ?login_error
- Password Transmitted over HTTP
- [Possible] Cross-site Request For
- HTTP Strict Transport Security (HSTS)
- faq.html
- help.html
- ?topic
- Cross-site Scripting via Remc
- [Possible] Source Code Disclo

Vulnerability | Browser View | HTTP Request / Response

Controlled Scan | Retest | Send to Request Builder | Generate WAF Rules | Execute SQL Commands | Get Shell | LFI Exploitation | Generate Exploit | Short Names

Out-of-date Version (OpenSSL)

CRITICAL

CERTAINTY

URL https://zero.webappsecurity.com/

IDENTIFIED VERSION 0.9.8e (contains 5 critical and 107 other vulnerabilities)

LATEST VERSION 3.0.0

VULNERABILITY DATABASE Result is based on 10-09-2021 vulnerability database content.

CLASSIFICATION

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
CAPEC	310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of OpenSSL.

IMPACT

Since this is an old version of the software, it may be vulnerable to attacks.

REMEDY

Vulnerability | Scan | Request Builder

Dashboard

Crawling & Attacking (2/3)...

90%

8915 / 9898

Scan Information

Current Speed:	14.2 req/sec
Average Speed:	14.4 req/sec
Total Requests:	12528
Failed Requests:	3
HEAD Requests:	557
Elapsed Time:	00:14:31

Issues (36)

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected
- [Possible] Source Code Disclosure (PHP)
- Insecure Transportation Security Protocol Supported (TLS 1.0)

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Issues (36) | Encoder | Logs (10)

Auto save finished successfully - 12-09-2021 20:30:26

Successfully updated vulnerability database to v2021.09.10.2030

Proxy: System

Type here to search

29°C ENG 20:38 12-09-2021

File View Reporting Tools Help

Start New Scan | Start Incremental Scan | Pause | Skip Current Phase | Import Links | Start Proxy

Site Map

- Out-of-date Version (jQu
- Out-of-date Version (Tomcat)
- Version Disclosure (Tomcat)
- search.html
- cgi-bin
- Forbidden Resource
- server-status
- Apache Server-Status Detected
- online-banking.html
- feedback.html
- [Possible] Cross-site Request For
- index.html
- login.html
- ?login_error
- Password Transmitted over HTTP
- [Possible] Cross-site Request For
- HTTP Strict Transport Security (HSTS
- faq.html
- help.html
- ?topic
- Cross-site Scripting via Remc
- [Possible] Source Code Disclo

Vulnerability | Browser View | HTTP Request / Response

Controlled Scan | Retest | Send to Request Builder | Generate WAF Rules | Execute SQL Commands | Get Shell | LFI Exploitation | Generate Exploit | Short Names

Out-of-date Version (Apache)

CRITICAL

CERTAINTY

URL https://zero.webappsecurity.com/

IDENTIFIED VERSION 2.2.6 (contains 4 critical and 65 other vulnerabilities)

LATEST VERSION 2.4.48

VULNERABILITY DATABASE Result is based on 10-09-2021 vulnerability database content.

CLASSIFICATION

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
CAPEC	310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of Apache.

IMPACT

Since this is an old version of the software, it may be vulnerable to attacks.

REMEDY

Vulnerability | Scan | Request Builder

Dashboard

Crawling & Attacking (2/3)...

96%

9300 / 9647

Scan Information

Current Speed:	14.3 req/sec
Average Speed:	14.3 req/sec
Total Requests:	13133
Failed Requests:	3
HEAD Requests:	557
Elapsed Time:	00:15:18

Issues (36)

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected
- [Possible] Source Code Disclosure (PHP)
- Insecure Transportation Security Protocol Supported (TLS 1.0)

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Issues (36) | Encoder | Logs (10)

Auto save finished successfully - 12-09-2021 20:30:26

Successfully updated vulnerability database to v2021.09.10.2030

Proxy: System

Type here to search

29°C ENG 20:39 12-09-2021

NetSparker's Detailed Scan Report

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	http://zero.webappsecurity.com/
SCAN DATE	12-09-2021 20:24:27
REPORT DATE	12-09-2021 20:34:46
SCAN DURATION	00:10:18
NETSPARKER VERSION	4.8.0.13139-master-20c2f1d

Total Requests
10355

Average Speed
16.73 req/sec.

36
Identified

10
Confirmed

3
Critical

11
Informational

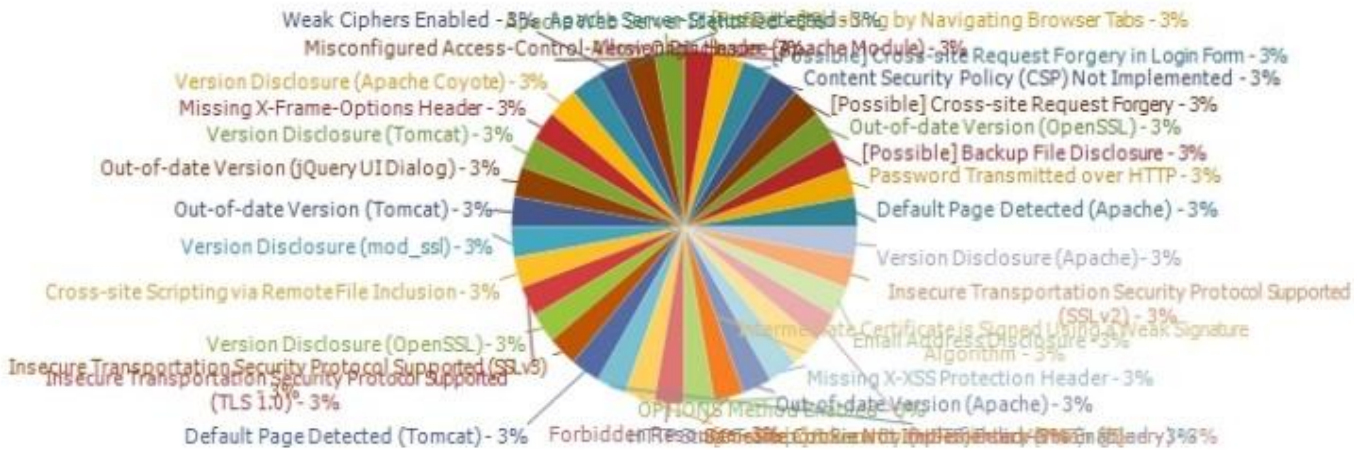
SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Server-Side Request Forgery (pattern based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)
URL REWRITE MODE	Heuristic
DETECTED URL REWRITE RULES	None

Authentication

Scheduled

VULNERABILITIES



CRITICAL
8%

IMPORTANT
8%

MEDIUM
17%

LOW
36%

INFORMATION
31%

1. Out-of-date Version (Tomcat)

1 TOTAL
CRITICAL

Netsparker identified you are using an out-of-date version of Tomcat.

Remedy

Please upgrade your installation of Tomcat to the latest stable version.

Remedy References

- Apache Tomcat Versions and Download

Known Vulnerabilities in this Version

Apache Tomcat Deserialization of Untrusted Data Vulnerability

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

External References

- CVE-2021-25329

Apache Tomcat Improper Authentication Vulnerability

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

External References

- CVE-2021-30640

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE

4. Password Transmitted over HTTP

1 TOTAL
IMPORTANT
CONFIRMED
1

Netsparker detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-319 CAPEC-65 WASC-4

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Base: 5.7 (Medium)
Temporal: 5.7 (Medium)
Environmental: 5.7 (Medium)

4.1. http://zero.webappsecurity.com/login.html Confirmed

http://zero.webappsecurity.com/login.html

Form target action

/signin.html

Request

```
GET /login.html HTTP/1.1
Host: zero.webappsecurity.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

5. Cross-site Scripting via Remote File Inclusion

1 TOTAL

IMPORTANT

CONFIRMED

1

Netsparker detected cross-site scripting via remote file inclusion, which makes it is possible to conduct cross-site scripting attacks by including arbitrary client-side dynamic scripts (*JavaScript, VBScript*).

Cross-site scripting allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application. This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by the user has been interpreted as HTML/JavaScript/VBScript by the browser.

Cross-site scripting targets the users of the application instead of the server. Although this is limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, Javascript or VbScript. To avoid this, all input and output from the application should be filtered. Output should be filtered according to the output format and location. Typically, the output location is HTML. Where the output is HTML, ensure all active content is removed prior to its presentation to the server.

My Report

- ***Title:-Critical Vulnerabilities Found By NetSparker***
- ***Domain:- webappsecurity.com***
- ***Subdomain:-http://zero.webappsecurity.com/***

Steps To Reproduce: 1.) Add Website you want to s to the dialogue box.

2.) Define the customization option to scan as per your need.

3.) It will start scanning it automatically.

4.) Choose any one of the Critical Vulnerabilities.

5.) Write Reports for the vulnerability you wanted to write. Make sure the report should not be the same as in Netsparker.

- ***Impact:- NetSparker identified 3 critical vulnerabilities which is out-of-date version. Since the software is of old version, it may be vulnerable to attacks.***
- ***Remedy:- The user should upgrade the installation of all the out-of-date version into the latest stable version so that it will be easy in using this website.***
- ***POC:- Screenshots of Vulnerability found.***