AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-8: Make a report of any vulnerability obtained by scanning any ip address

REPORT

VULNERABILITY NAME: APACHE TOMCAT

CWE: CWE-444- Inconsistent Interpretation of HTTP Requests ('HTTP Request / Response Smuggling')

OWASP Category: A04:2021 - Insecure Design

DESCRIPTION: The product acts as an intermediary HTTP agent (such as a proxy or firewall) in the data flow between two entities such as a client and server, but it does not interpret malformed HTTP requests or responses in ways that are consistent with how the messages will be processed by those entities that are at the ultimate destination.

Description about the vulnerability: The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities. An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)

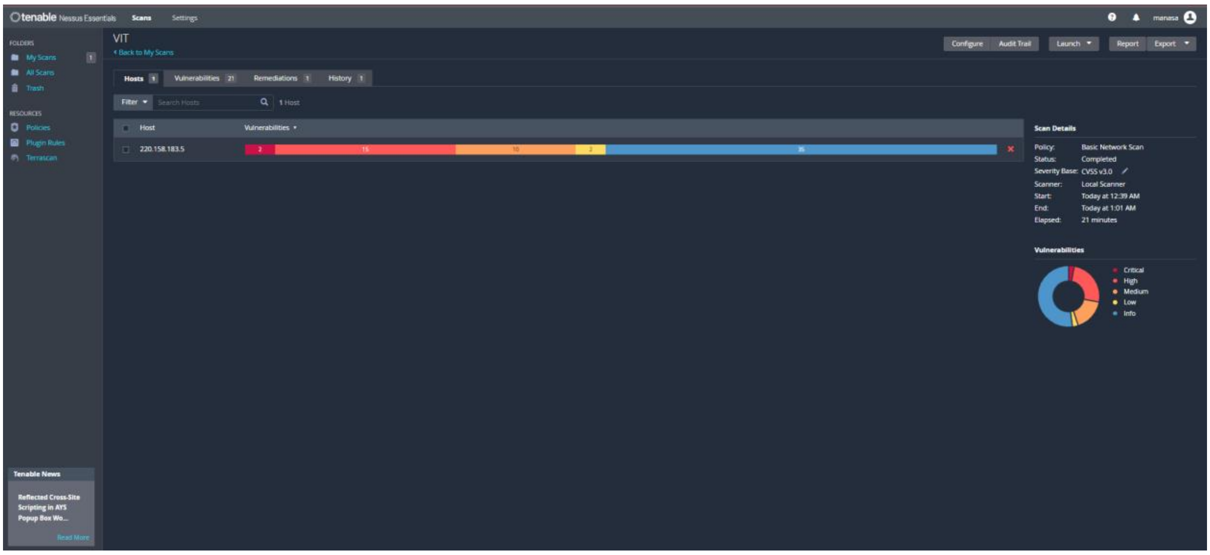
BUSINESS IMPACT: Exploiting this vulnerability may lead to unauthorized access, exposing sensitive customer data and damaging a company's reputation. Attackers can disrupt web services, causing downtime and affecting customer experience, leading to loss of revenue and customer trust. Non-compliance with data protection regulations (e.g., GDPR) can result in hefty fines, legal actions, and reputational damage. Businesses may face financial losses due to cleanup costs, customer compensation, and increased security investments. Repeated incidents can erode customer trust, leading to reduced customer loyalty and market share.

CVSS Score: 9.8

This means this vulnerability has high risk factor and the severity is critical.

AFFECTED URL: https://vtop2.vitap.ac.in

POC (PROOF OF CONCEPT):



VIT

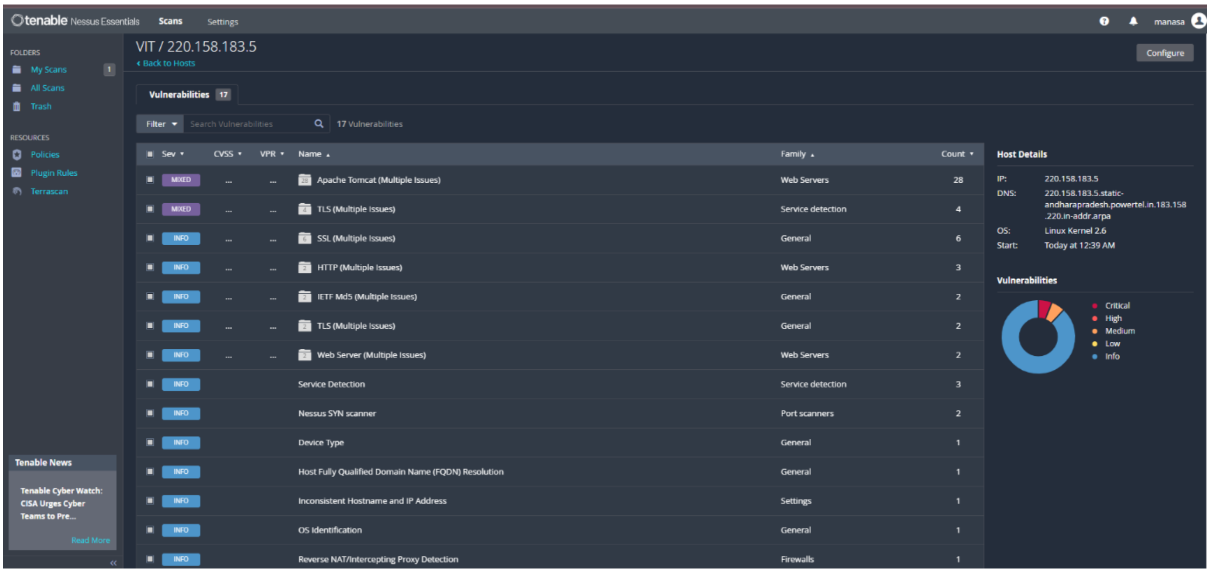
Host	Vulnerabilities
220.158.183.5	2 15 10 2 35

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:39 AM
End: Today at 1:01 AM
Elapsed: 21 minutes

Tenable News

Reflected Cross-Site Scripting in AYS Popup Box Wo...



VIT / 220.158.183.5

‹ Back to Hosts

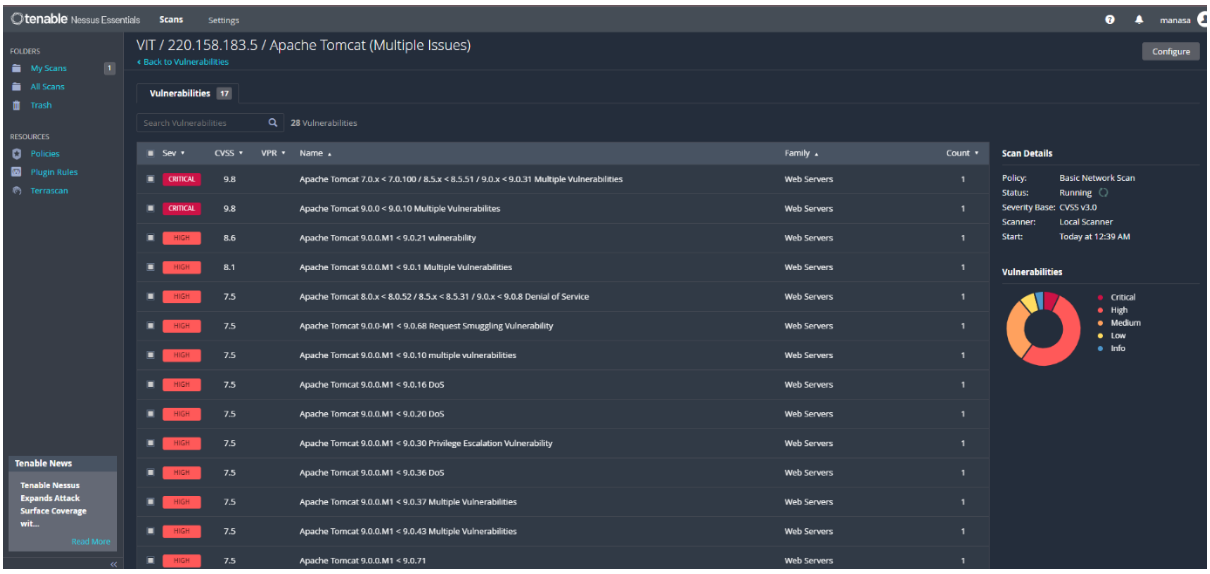
17 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	28 Apache Tomcat (Multiple Issues)	Web Servers	28
MIXED	...	...	4 TLS (Multiple Issues)	Service detection	4
INFO	...	...	6 SSL (Multiple Issues)	General	6
INFO	...	...	3 HTTP (Multiple Issues)	Web Servers	3
INFO	...	...	2 IETF Md5 (Multiple Issues)	General	2
INFO	...	...	2 TLS (Multiple Issues)	General	2
INFO	...	...	2 Web Server (Multiple Issues)	Web Servers	2
INFO			Service Detection	Service detection	3
INFO			Nessus SYN scanner	Port scanners	2
INFO			Device Type	General	1
INFO			Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO			Inconsistent Hostname and IP Address	Settings	1
INFO			OS Identification	General	1
INFO			Reverse NAT/Intercepting Proxy Detection	Firewalls	1

Host Details

IP:	220.158.183.5
DNS:	220.158.183.5.static-andharapradesh.powertel.in.183.158.220.in-addr.arpa
OS:	Linux Kernel 2.6
Start:	Today at 12:39 AM

Vulnerabilities



VIT / 220.158.183.5 / Apache Tomcat (Multiple Issues)

‹ Back to Vulnerabilities

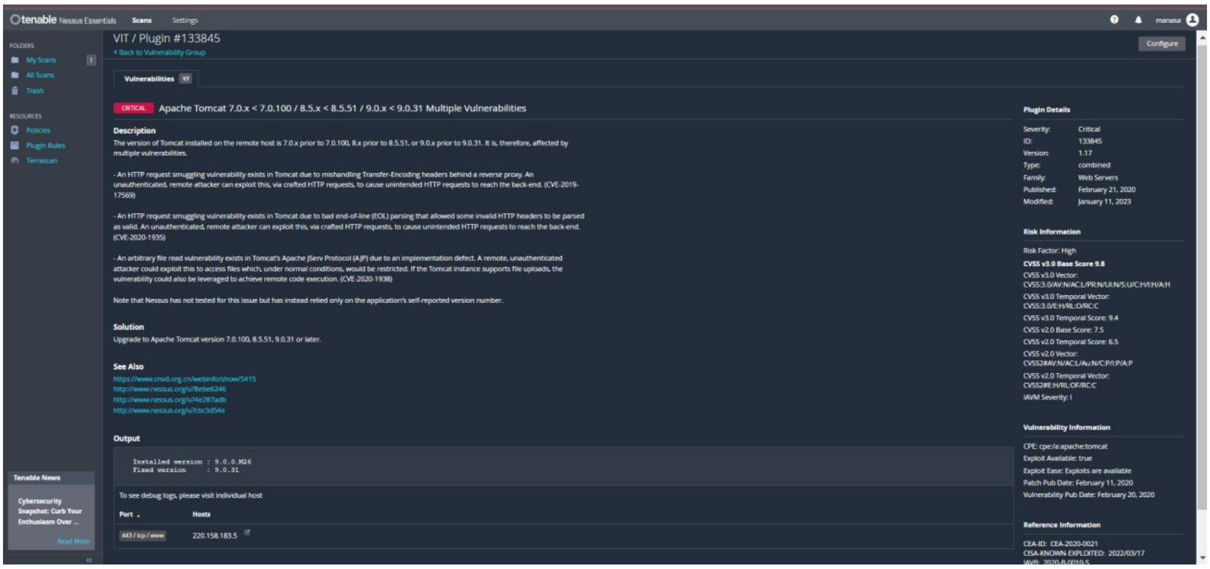
28 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.8		Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilites	Web Servers	1
HIGH	8.6		Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability	Web Servers	1
HIGH	8.1		Apache Tomcat 9.0.0.M1 < 9.0.1 Multiple Vulnerabilities	Web Servers	1
HIGH	7.5		Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.10 multiple vulnerabilities	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.16 DoS	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.20 DoS	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.36 DoS	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities	Web Servers	1
HIGH	7.5		Apache Tomcat 9.0.0.M1 < 9.0.71	Web Servers	1

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:39 AM

Vulnerabilities



VIT / Plugin #133845

‹ Back to Vulnerability Group

CRITICAL Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities

Description

The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.

- An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)

- An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)

- An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later.

See Also

https://www.cnvd.org.cn/webinfo/show/5415
http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e

Output

```
  Installed version : 9.0.0.M26
  Fixed version     : 9.0.31
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	220.158.183.5

Plugin Details

Severity:	Critical
ID:	133845
Version:	1.17
Type:	combined
Family:	Web Servers
Published:	February 21, 2020
Modified:	January 11, 2023

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 6.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: February 11, 2020
Vulnerability Pub Date: February 20, 2020

Reference Information

CEA-ID: CEA-2020-0021
CISA-KNOWN-EXPLOITED: 2022/03/17
IAVB: 2020-B-0010-S

REMEDIATION:

Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later. Upgradation to further versions can solve the issue.