TITLE: Malware Detection and Classification

TEAM NUMBER: 2.5

TEAM MEMBERS:

- Hardik Kankane
- Anondita Dutta
- Elisabeth Varghese

Vulnerability Report

Target IP 1: 182.73.197.23

1. Nessus SYN scanner

CWE: N/A

OWASP Category: N/A

Description: Nessus SYN scanner is a plugin used for network scanning.

Business Impact: Informational plugin for network discovery.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

2. Nessus Scan Information

CWE: N/A

OWASP Category: N/A

Description: Information about the Nessus scan itself.

Business Impact: Provides information about the scan process.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

3. OS Identification Failed

CWE: N/A

OWASP Category: N/A

Description: Nessus failed to identify the operating system.

Business Impact: May affect vulnerability assessment.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

4. Open Port Re-check

CWE: N/A

OWASP Category: N/A

Description: Nessus re-checks open ports.

Business Impact: Informational plugin for port status.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

5. Service Detection

CWE: N/A

OWASP Category: N/A

Description: Plugin used to detect services running on open ports.

Business Impact: Provides information about running services.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

6. Traceroute Information

CWE: N/A

OWASP Category: N/A

Description: Provides information about the traceroute.

Business Impact: Informational plugin for network mapping.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

7. Web Server No 404 Error Code Check

CWE: N/A

OWASP Category: N/A

Description: Checks for the absence of 404 error codes on the web server.

Business Impact: Informational plugin for web server analysis.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

Target IP 2: 14.99.16.249

1. Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability

CWE: CWE-444

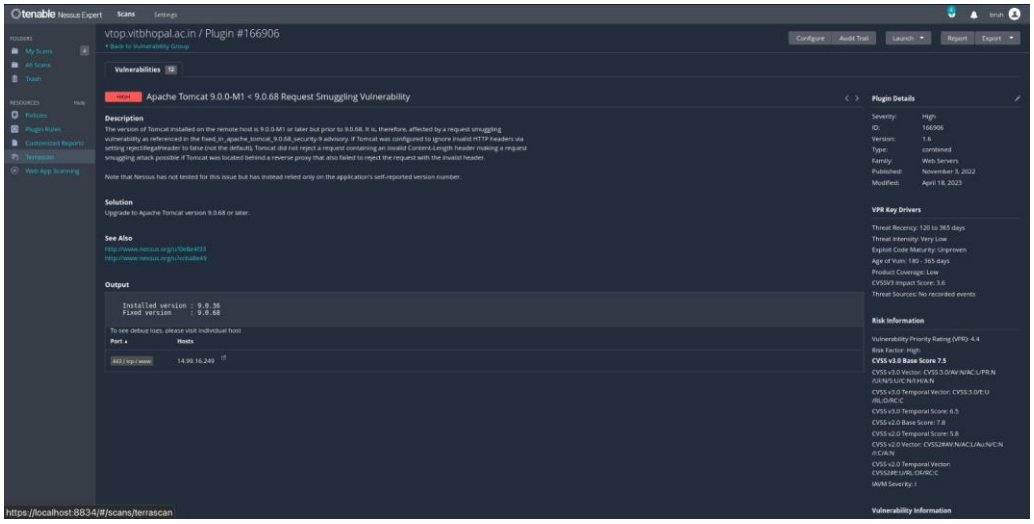
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat version 9.0.0-M1 to 9.0.68 allows an attacker to perform request smuggling attacks.

Business Impact: Potential for HTTP request smuggling leading to unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



2. Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities

CWE: CWE-444

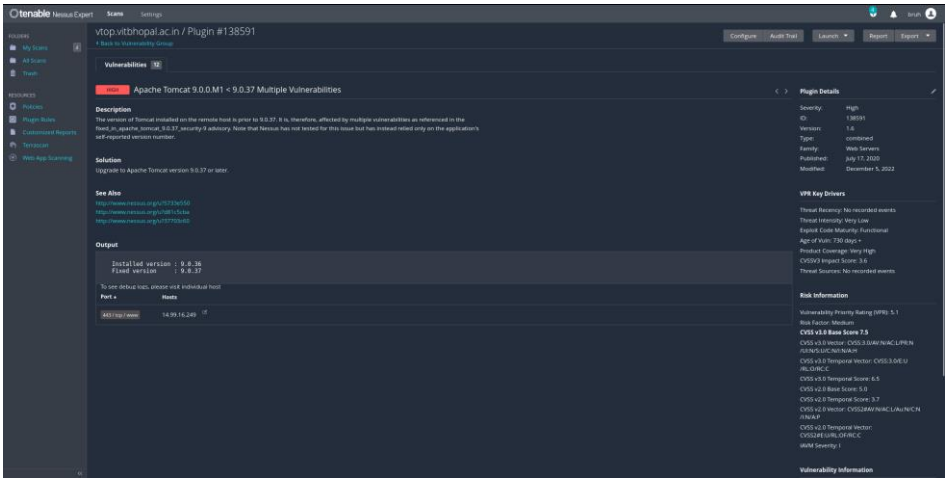
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.37 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



3. Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities

CWE: CWE-444

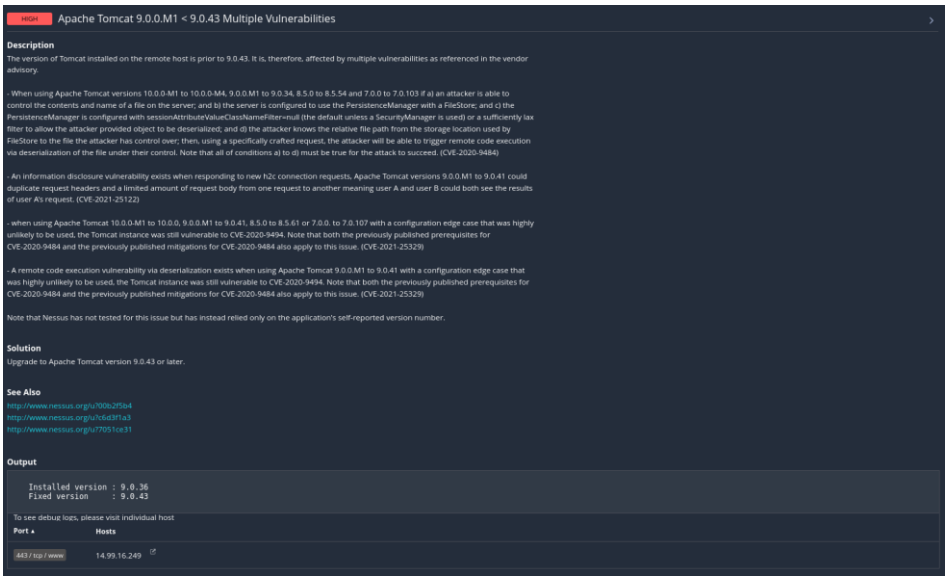
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.43 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



4. Apache Tomcat 9.0.0.M1 < 9.0.71

CWE: CWE-444

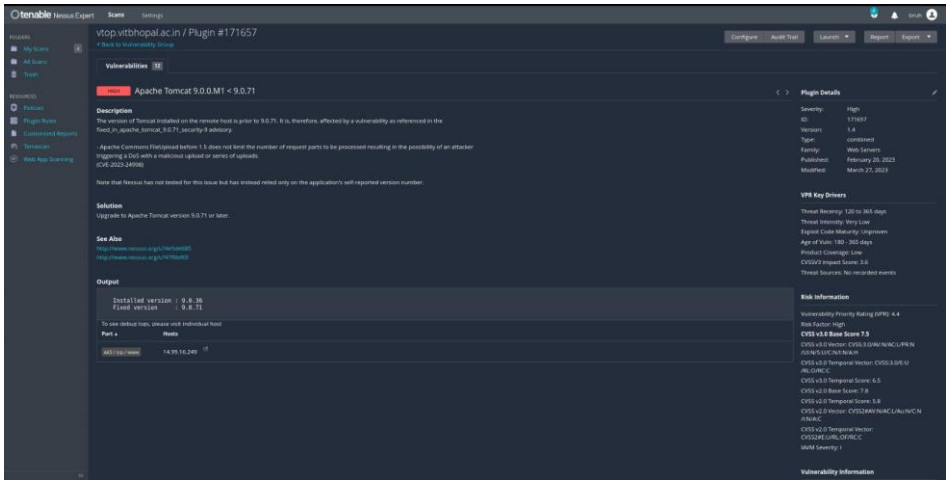
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.71 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



5. Apache Tomcat 9.0.13 < 9.0.63 Vulnerability

CWE: CWE-444

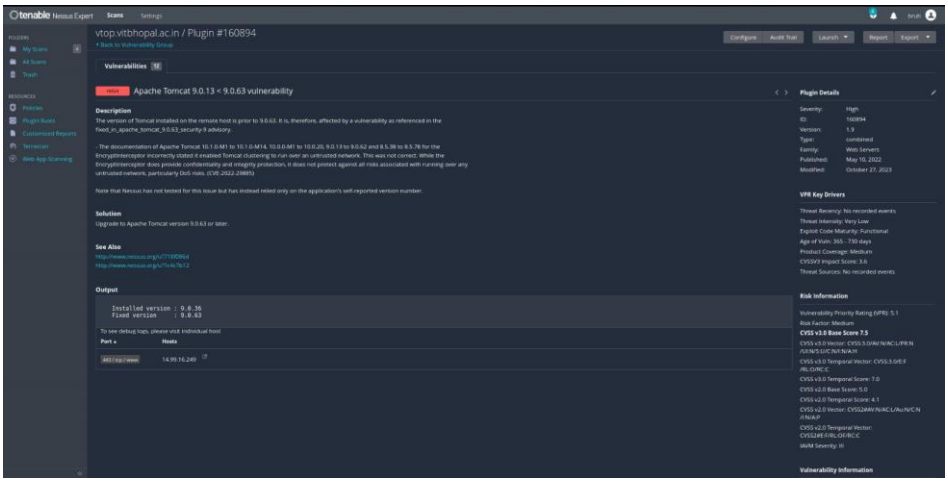
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.13 through 9.0.63 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



6. Apache Tomcat 9.0.0.M1 < 9.0.80

CWE: CWE-444

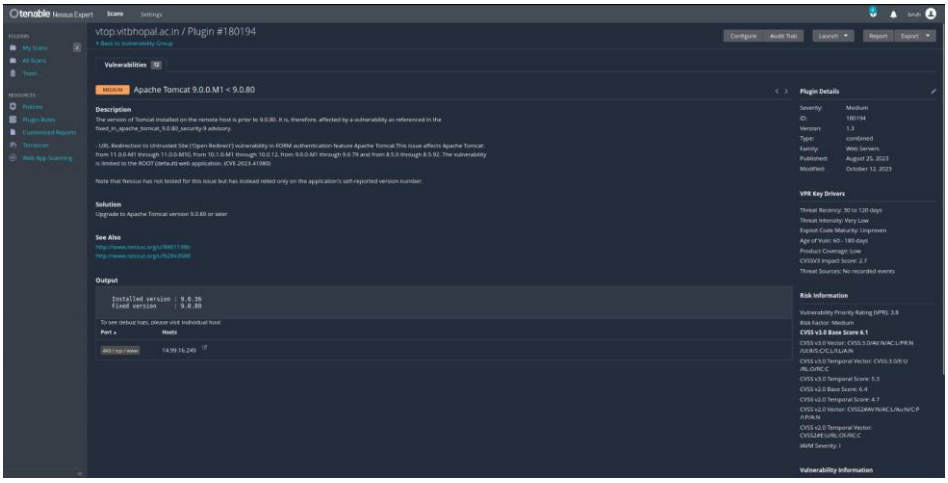
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.80 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



7. Apache Tomcat 9.0.30 < 9.0.65 Vulnerability

CWE: CWE-444

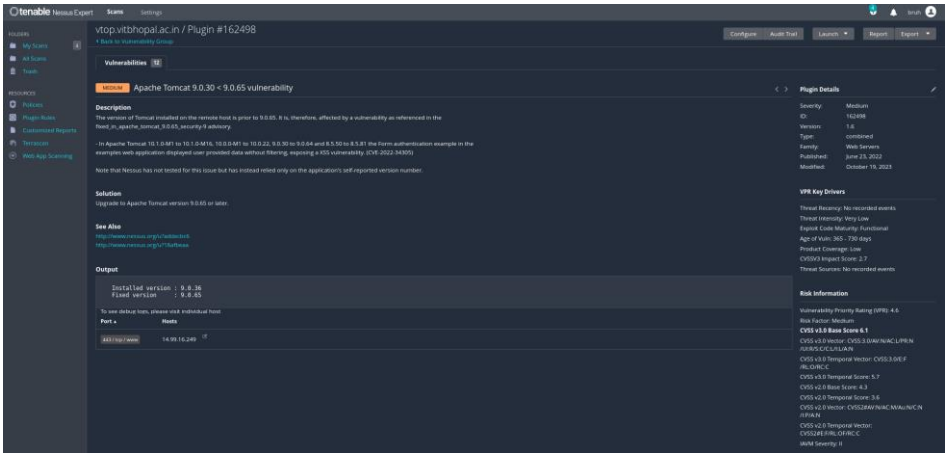
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.30 through 9.0.65 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



8. Apache Tomcat 9.0.0.M1 < 9.0.48 Vulnerability

CWE: CWE-444

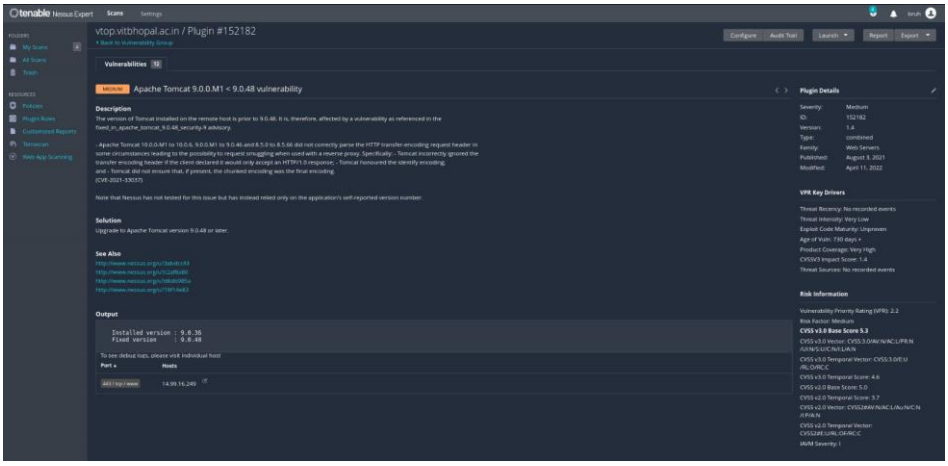
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.48 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



9. Apache Tomcat 9.0.0.M1 < 9.0.81 Multiple Vulnerabilities

CWE: CWE-444

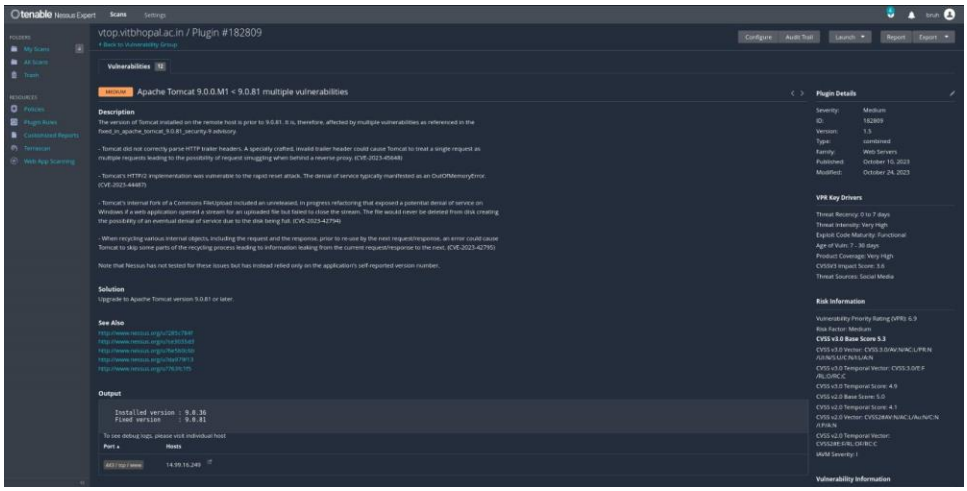
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.81 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



10. Apache Tomcat 9.0.0.M1 < 9.0.72

CWE: CWE-444

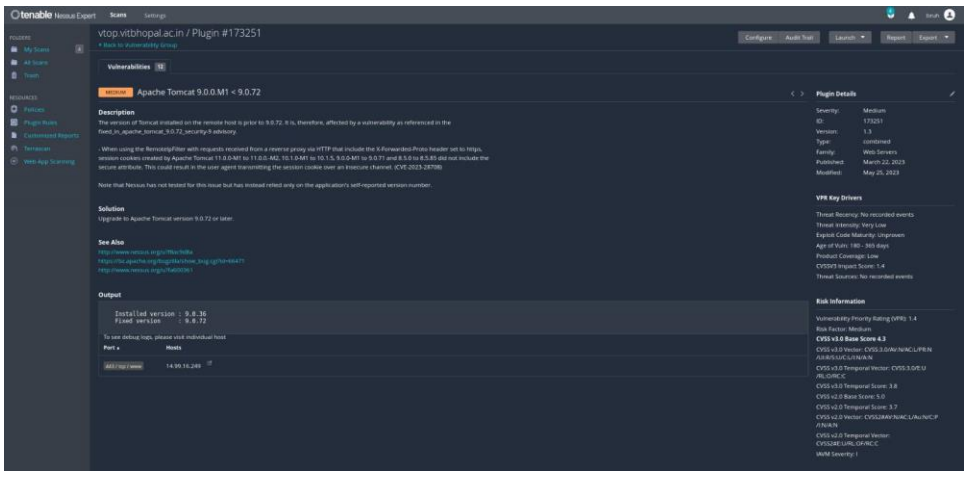
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.72 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



11. Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations

CWE: CWE-444

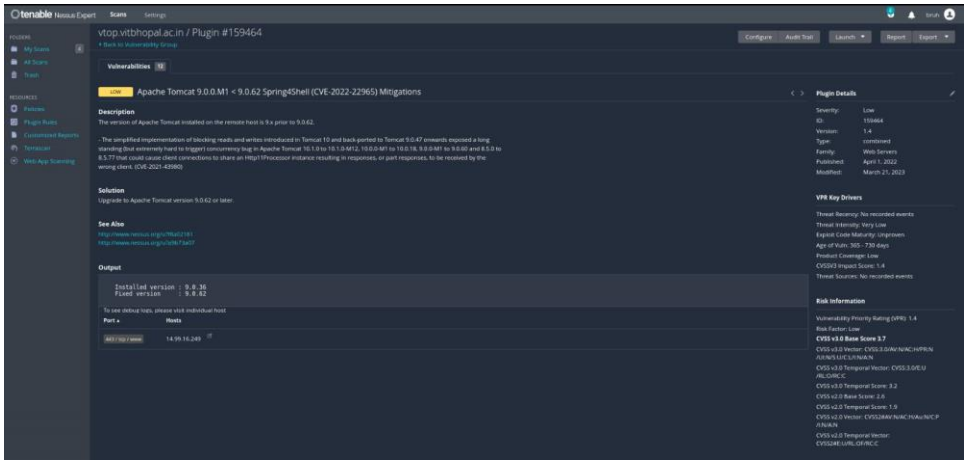
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Mitigations for the Spring4Shell vulnerability (CVE-2022-22965) in Apache Tomcat versions 9.0.0.M1 through 9.0.62.

Business Impact: Provides mitigations for a critical vulnerability.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.



12. Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

CWE: CWE-444

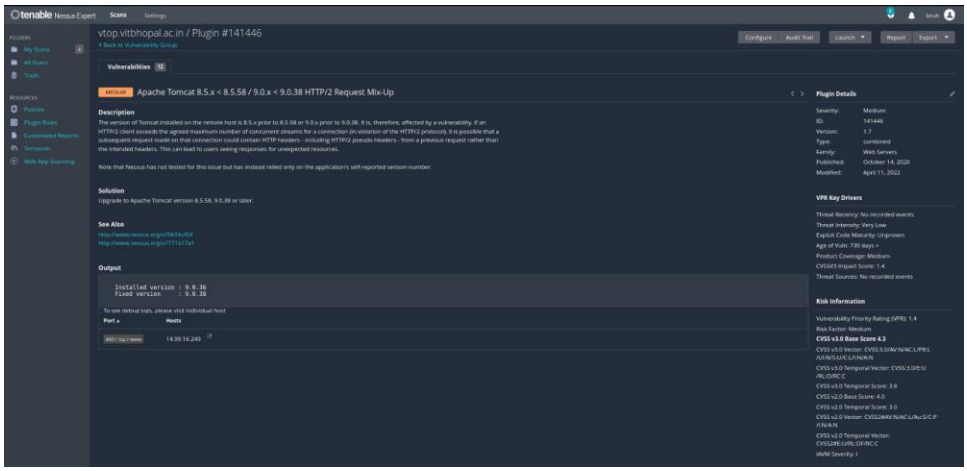
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 8.5.x through 8.5.58 and 9.0.x through 9.0.38 may allow attackers to conduct HTTP/2 request mix-up attacks.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/


tenable Nessus Expert
Scans
Settings
vtop.vitbhopal.ac.in / Plugin #141446
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 12
MEDIUM
Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up
Description
Solution
Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later.
See Also
Output
Installed version : 9.0.36
Fixed version : 9.0.38
To see debug logs, please visit individual host
Port
Hosts
14.99.16.249
Plugin Details
Severity: Medium
ID: 141446
Version: 1.7
Type: combined
Family: Web Servers
Published: October 14, 2020
Modified: April 11, 2022
VPR Key Drivers
Risk Information
Vulnerability Priority Rating (VPR): 1.4
Risk Factor: Medium
CVSS v3.0 Base Score 4.3