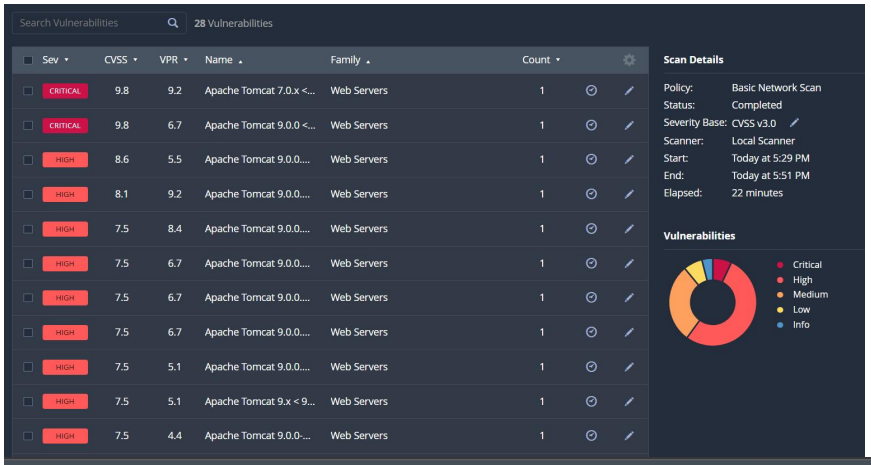
Task 8:

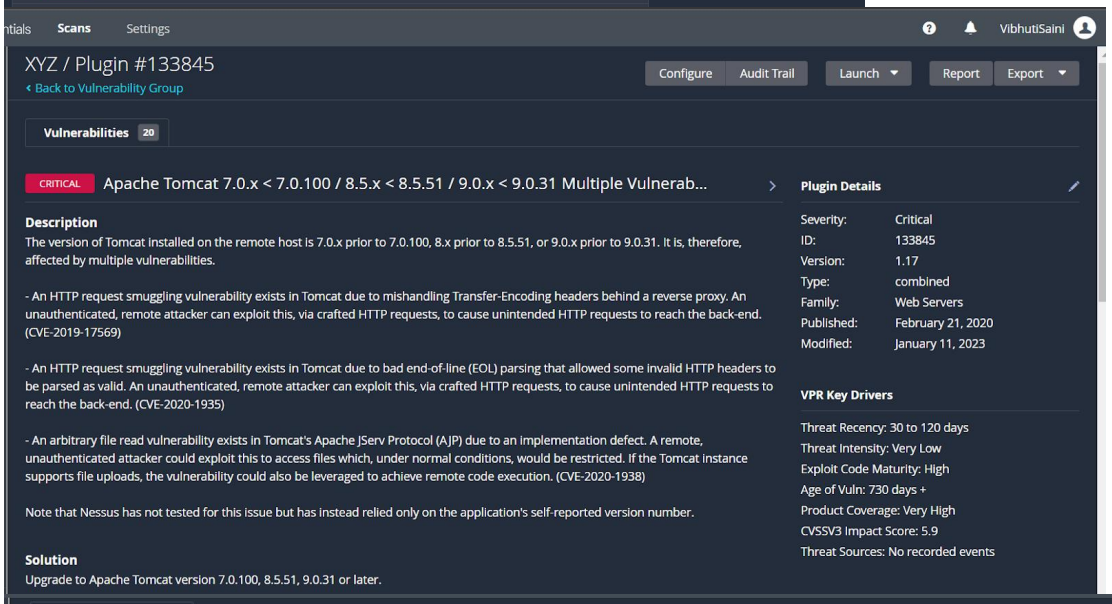
Report Procedure:

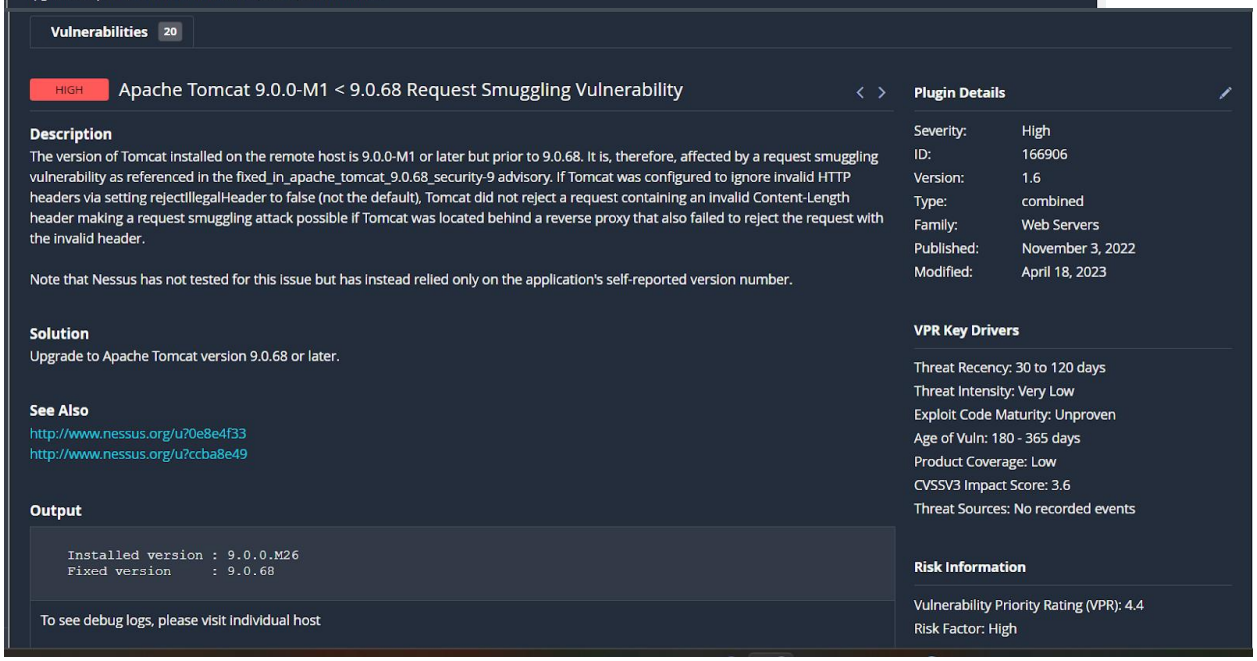
Vulnerability Name: Broken Access Control
CWE:CWE 400,CWE 770
OWASP: Allocation of Resources without limits or throttling
Description: The HTTP/2 implementation accepted streams with excessive numbers of SETTINGS frames and also permitted clients to keep streams open without reading/writing requests/response data.By keeping streams open for requests that utilized the Servlet API's blocking I/O,client were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS
Business Impact: This type of attack that prevents the users from getting access to the systems.Giving any user authorization to perform such a task which they are not supposed to will result in information exposure, dos(denial of service) and arbitrary code execution.
Affected URL:
URL:https://vtop2.vitap.ac.in/vtop/initialProcess

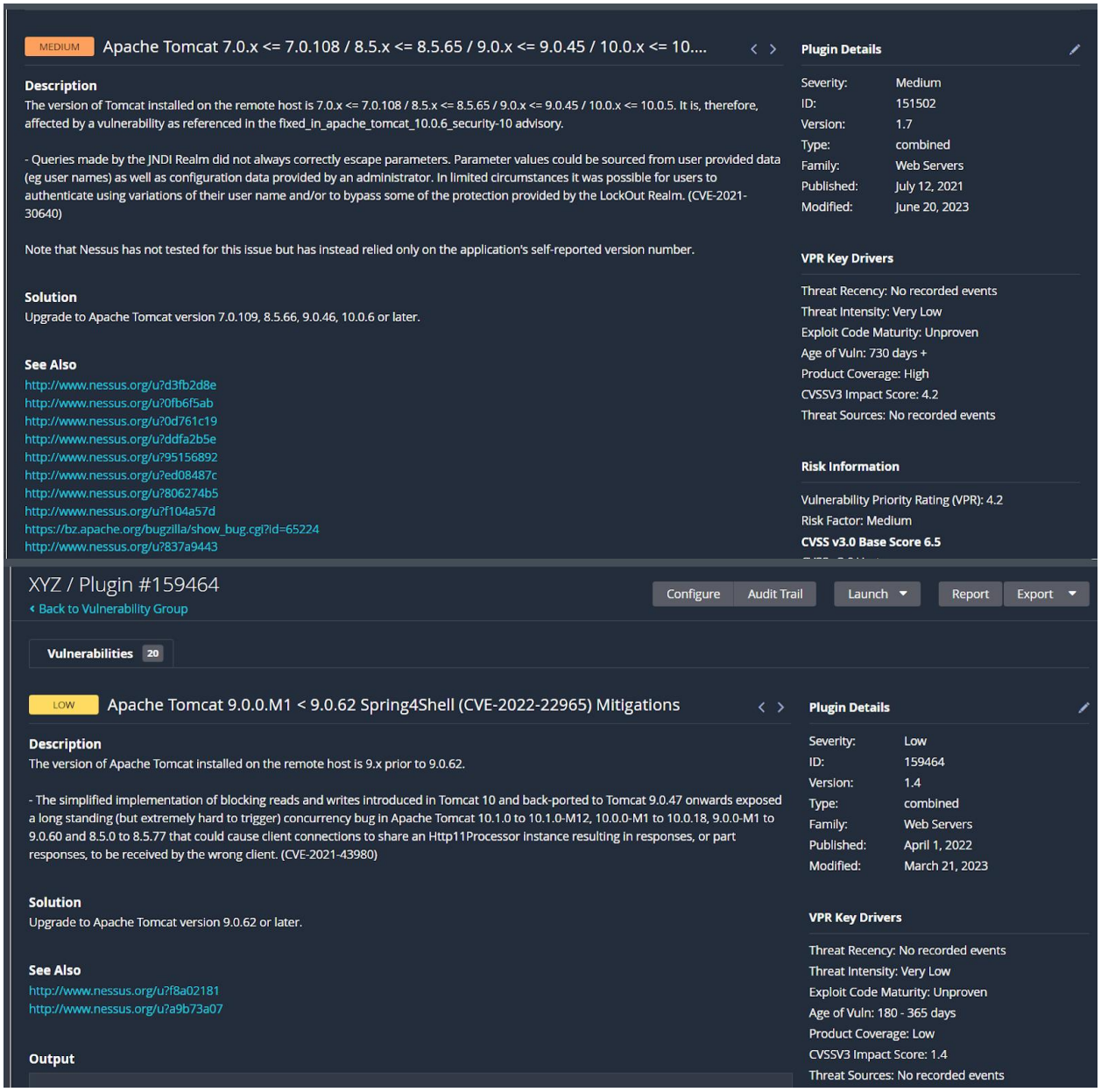
IPv4:220.158.183.5

POC(Proof of concept):


Search Vulnerabilities
28 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL 9.8 9.2 Apache Tomcat 7.0.x <... Web Servers 1
CRITICAL 9.8 6.7 Apache Tomcat 9.0.0 <... Web Servers 1
HIGH 8.6 5.5 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 8.1 9.2 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 8.4 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 6.7 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 6.7 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 6.7 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 5.1 Apache Tomcat 9.0.0.... Web Servers 1
HIGH 7.5 5.1 Apache Tomcat 9.x < 9... Web Servers 1
HIGH 7.5 4.4 Apache Tomcat 9.0.0-... Web Servers 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:29 PM
End: Today at 5:51 PM
Elapsed: 22 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


tials
Scans
Settings
VibhutiSaini
XYZ / Plugin #133845
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 20
CRITICAL Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerab...
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.
Plugin Details
Severity: Critical
ID: 133845
Version: 1.17
Type: combined
Family: Web Servers
Published: February 21, 2020
Modified: January 11, 2023
VPR Key Drivers
Threat Recency: 30 to 120 days
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events


Vulnerabilities 20
HIGH Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability
Description
The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed_in_apache_tomcat_9.0.68_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.
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 9.0.68 or later.
See Also
http://www.nessus.org/u?0e8e4f33
http://www.nessus.org/u?ccba8e49
Output
Installed version : 9.0.0.M26
Fixed version : 9.0.68
To see debug logs, please visit individual host
Plugin Details
Severity: High
ID: 166906
Version: 1.6
Type: combined
Family: Web Servers
Published: November 3, 2022
Modified: April 18, 2023
VPR Key Drivers
Threat Recency: 30 to 120 days
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 180 - 365 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 4.4
Risk Factor: High


MEDIUM
Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10....
Description
The version of Tomcat installed on the remote host is 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_10.0.6_security-10 advisory.
- Queries made by the JNDI Realm did not always correctly escape parameters. Parameter values could be sourced from user provided data (eg user names) as well as configuration data provided by an administrator. In limited circumstances it was possible for users to authenticate using variations of their user name and/or to bypass some of the protection provided by the LockOut Realm. (CVE-2021-30640)
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 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later.
See Also
http://www.nessus.org/u?d3fb2d8e
http://www.nessus.org/u?0fb6f5ab
http://www.nessus.org/u?0d761c19
http://www.nessus.org/u?ddfa2b5e
http://www.nessus.org/u?95156892
http://www.nessus.org/u?ed08487c
http://www.nessus.org/u?806274b5
http://www.nessus.org/u?f104a57d
https://bz.apache.org/bugzilla/show_bug.cgi?id=65224
http://www.nessus.org/u?837a9443
Plugin Details
Severity: Medium
ID: 151502
Version: 1.7
Type: combined
Family: Web Servers
Published: July 12, 2021
Modified: June 20, 2023
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 4.2
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 4.2
Risk Factor: Medium
CVSS v3.0 Base Score 6.5
XYZ / Plugin #159464
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 20
LOW
Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations
Description
The version of Apache Tomcat installed on the remote host is 9.x prior to 9.0.62.
- The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client. (CVE-2021-43980)
Solution
Upgrade to Apache Tomcat version 9.0.62 or later.
See Also
http://www.nessus.org/u?f8a02181
http://www.nessus.org/u?a9b73a07
Output
Plugin Details
Severity: Low
ID: 159464
Version: 1.4
Type: combined
Family: Web Servers
Published: April 1, 2022
Modified: March 21, 2023
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 180 - 365 days
Product Coverage: Low
CVSSV3 Impact Score: 1.4
Threat Sources: No recorded events