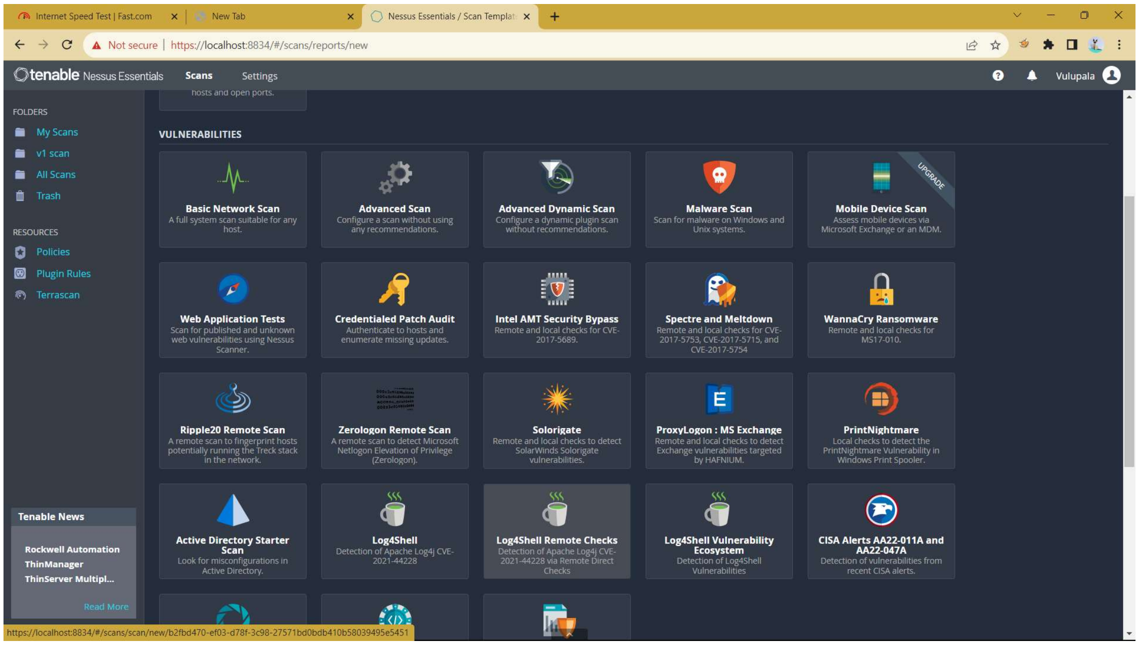
NESSUSS: is a web client vulnerability scanner used to scan all the possible vulnerability that present in the given host(IP address)

Step wise analysis report generated on HOST scan (10.10.0.1)

There are various types of vulnerability scans available on Nessus web client application as shown below:


Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Scan Templat
Not secure
https://localhost:8834/#/scans/reports/new
tenable Nessus Essentials
Scans
Settings
Vulupala
hosts and open ports.
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.
Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.
Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.
Tenable News
Rockwell Automation ThinManager ThinServer Multipl...
Read More
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Log4Shell
Detection of Apache Log4j CVE-2021-44228
Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks
Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities
CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.
https://localhost:8834/#/scans/scan/new/b2fbd470-ef03-d78f-3c98-27571bd0bdb410b58039495e5451

- ➢ Each of these scans have there own method to find vulnerabilities and other kind of attacks that could be append on the host.
- ➢ In this particular vulnerability scan we are applying “Basic Network Scan”

  STEP 1:

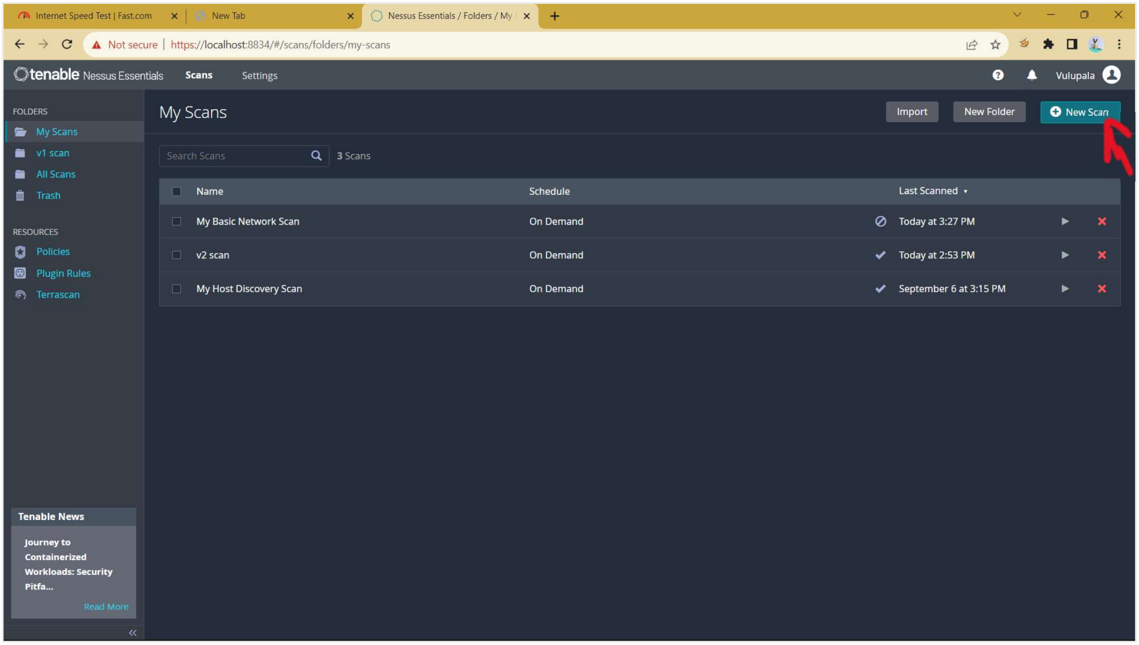
  Login to the Nessus using the login credentials created used at the time of registering.

  STEP 2:

  After complete installation of plugins we will start the basic network scan

  STEP 3:

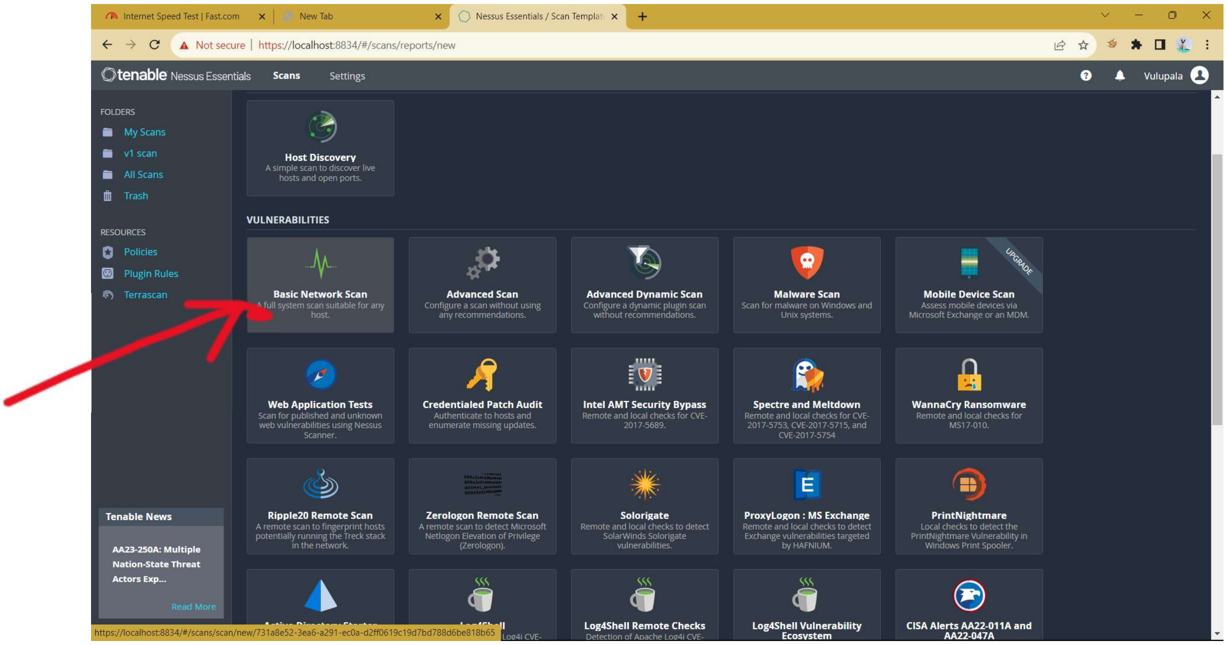
  Select New scan :



Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Folders / My
Not secure | https://localhost:8834/#/scans/folders/my-scans
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Journey to Containerized Workloads: Security Pitfa...
Read More
My Scans
Import
New Folder
New Scan
Search Scans
3 Scans

Name	Schedule	Last Scanned
My Basic Network Scan	On Demand	Today at 3:27 PM
v2 scan	On Demand	Today at 2:53 PM
My Host Discovery Scan	On Demand	September 6 at 3:15 PM

STEP 4: Select Basic Network scan



Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Scan Templat
Not secure | https://localhost:8834/#/scans/reports/new
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
AA23-250A: Multiple Nation-State Threat Actors Exp...
Read More
VULNERABILITIES
UPGRADE
https://localhost:8834/#/scans/scan/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

Host Discovery A simple scan to discover live hosts and open ports.

Basic Network Scan A full system scan suitable for any host.

Advanced Scan Configure a scan without using any recommendations.

Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Malware Scan Scan for malware on Windows and Unix systems.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware Remote and local checks for MS17-010.

Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter

Log4Shell Log4j CVE-

Log4Shell Remote Checks Detection of Apache Log4j CVE-

Log4Shell Vulnerability Ecosystem

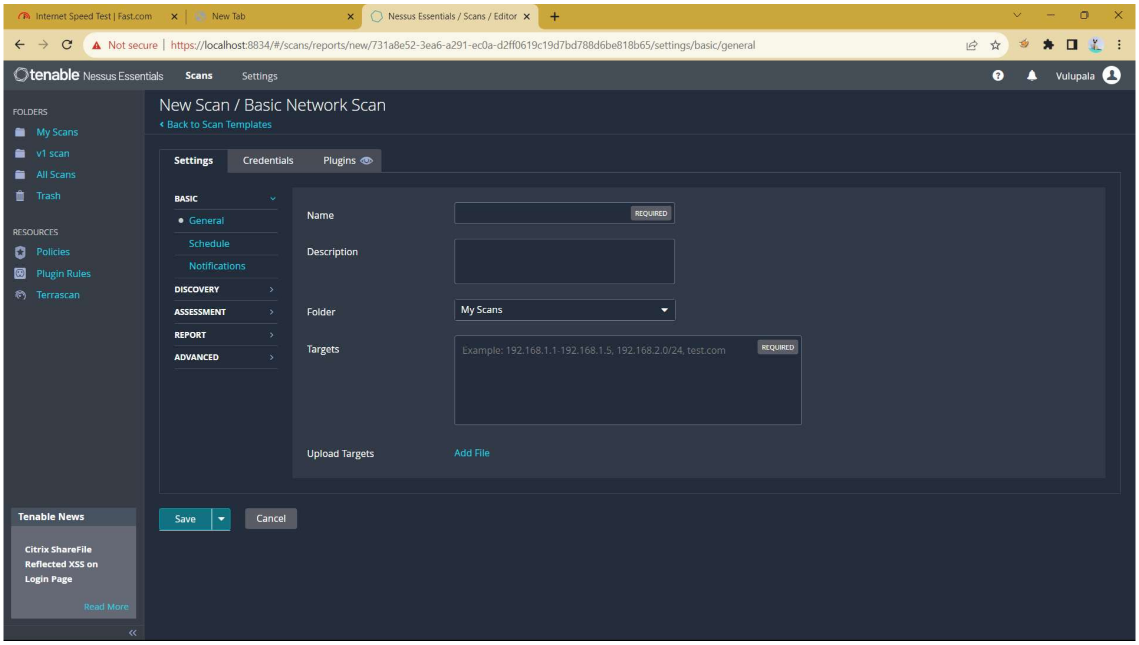
CISA Alerts AA22-011A and AA22-047A

- ➢ Basic Network scan provide vulnerability details such as :

1. Software flaws
2. ,missing patches
3. Misconfigurations

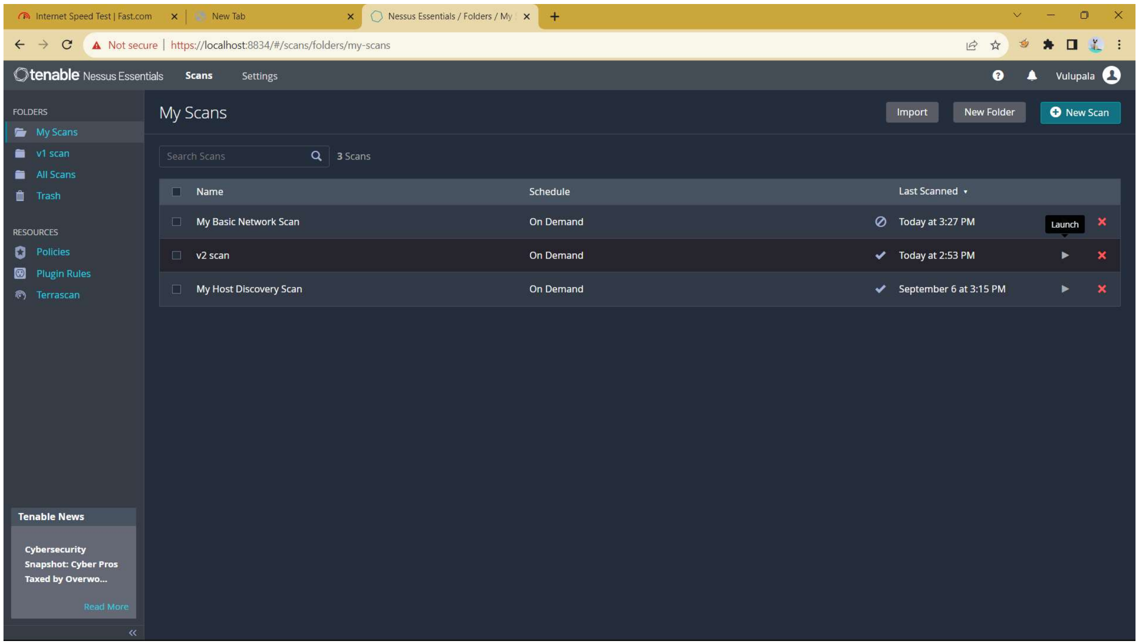
4. Denial of service vulnerabilities
5. Default passwords

STEP 5: Enter the scan details :


Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Scans / Editor
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel
Tenable News
Citrix ShareFile Reflected XSS on Login Page
Read More

- ➢ Enter the name of the scan :
- ➢ Enter the target IP address or URL
- ➢ Save the details of the your scan using save button.

STEP 6:

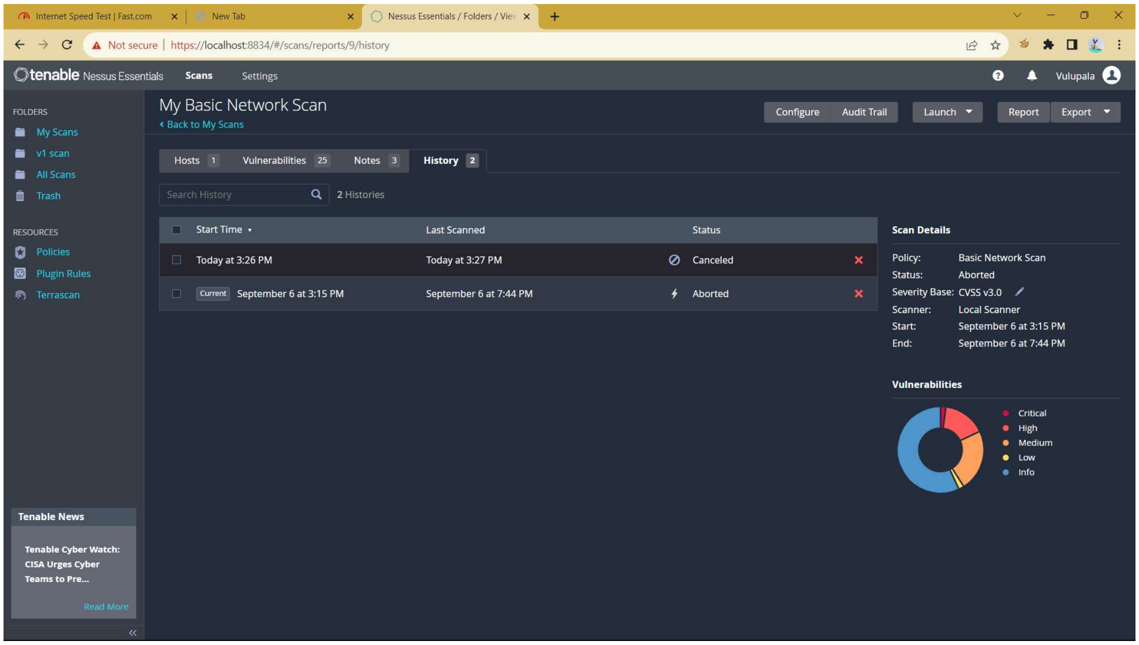


Name	Schedule	Last Scanned
My Basic Network Scan	On Demand	Today at 3:27 PM
v2 scan	On Demand	Today at 2:53 PM
My Host Discovery Scan	On Demand	September 6 at 3:15 PM

- You will be able to see your host name details. Click on lunch button to lunch your vulnerability scan.
- The scanning procedure may take time according to the internet availability

  Approximately : 1-2 hr for a complete scan

STEP 7:



My Basic Network Scan

‹ Back to My Scans

2 Histories

Start Time	Last Scanned	Status
Today at 3:26 PM	Today at 3:27 PM	Canceled
Current September 6 at 3:15 PM	September 6 at 7:44 PM	Aborted

Scan Details

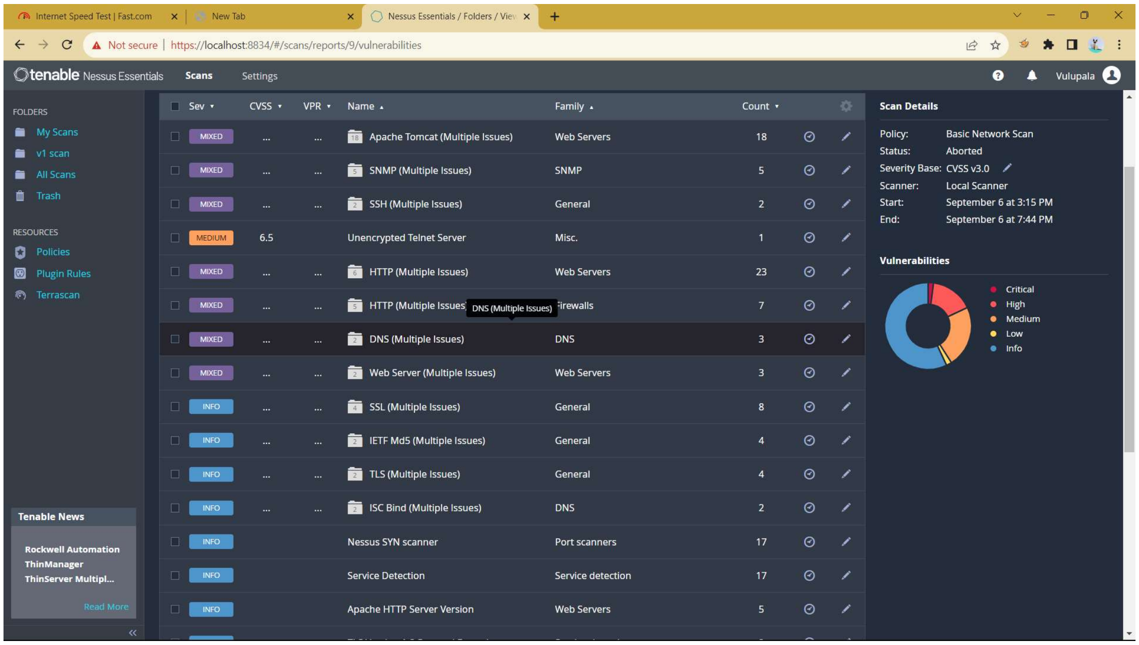
Policy:	Basic Network Scan
Status:	Aborted
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	September 6 at 3:15 PM
End:	September 6 at 7:44 PM

Vulnerabilities

Once the scan finishes you will be able to find the vulnerability report as shown in the above figure

To know complete details of the scan click on the report generated.

STEP 8:


Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Folders / View
Not secure | https://localhost:8834/#/scans/reports/9/vulnerabilities
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Rockwell Automation ThinManager ThinServer Multipl...
Read More
DNS (Multiple Issues)
Critical
High
Medium
Low
Info

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	18 Apache Tomcat (Multiple Issues)	Web Servers	18
MIXED	...	...	5 SNMP (Multiple Issues)	SNMP	5
MIXED	...	...	2 SSH (Multiple Issues)	General	2
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1
MIXED	...	...	6 HTTP (Multiple Issues)	Web Servers	23
MIXED	...	...	5 HTTP (Multiple Issues)	Firewalls	7
MIXED	...	...	2 DNS (Multiple Issues)	DNS	3
MIXED	...	...	2 Web Server (Multiple Issues)	Web Servers	3
INFO	...	...	4 SSL (Multiple Issues)	General	8
INFO	...	...	2 IETF Md5 (Multiple Issues)	General	4
INFO	...	...	2 TLS (Multiple Issues)	General	4
INFO	...	...	2 ISC Bind (Multiple Issues)	DNS	2
INFO			Nessus SYN scanner	Port scanners	17
INFO			Service Detection	Service detection	17
INFO			Apache HTTP Server Version	Web Servers	5

Scan Details

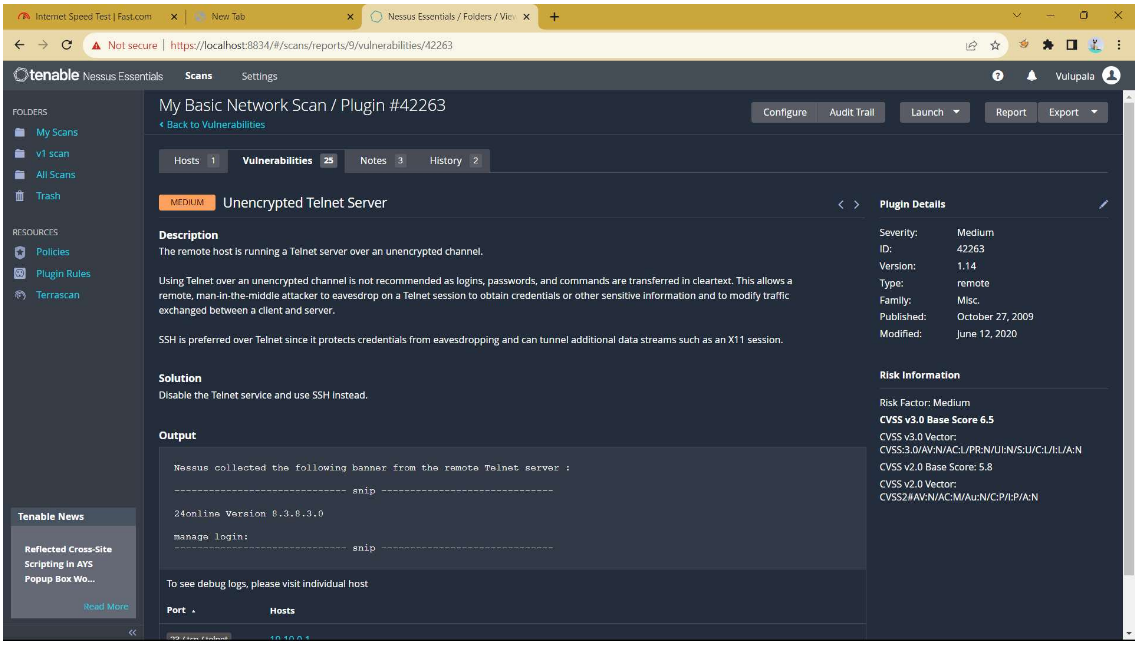
Policy:	Basic Network Scan
Status:	Aborted
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	September 6 at 3:15 PM
End:	September 6 at 7:44 PM

Vulnerabilities

- These are the some of vulnerabilities the scan could find to know in details click on

  The vulnerability to want

  Below are some the examples:



My Basic Network Scan / Plugin #42263

‹ Back to Vulnerabilities

MEDIUM Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Output

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------

24online Version 8.3.8.3.0

manage login:
------------------------------ snip ------------------------------
```

To see debug logs, please visit individual host

Plugin Details

Severity:	Medium
ID:	42263
Version:	1.14
Type:	remote
Family:	Misc.
Published:	October 27, 2009
Modified:	June 12, 2020

Risk Information

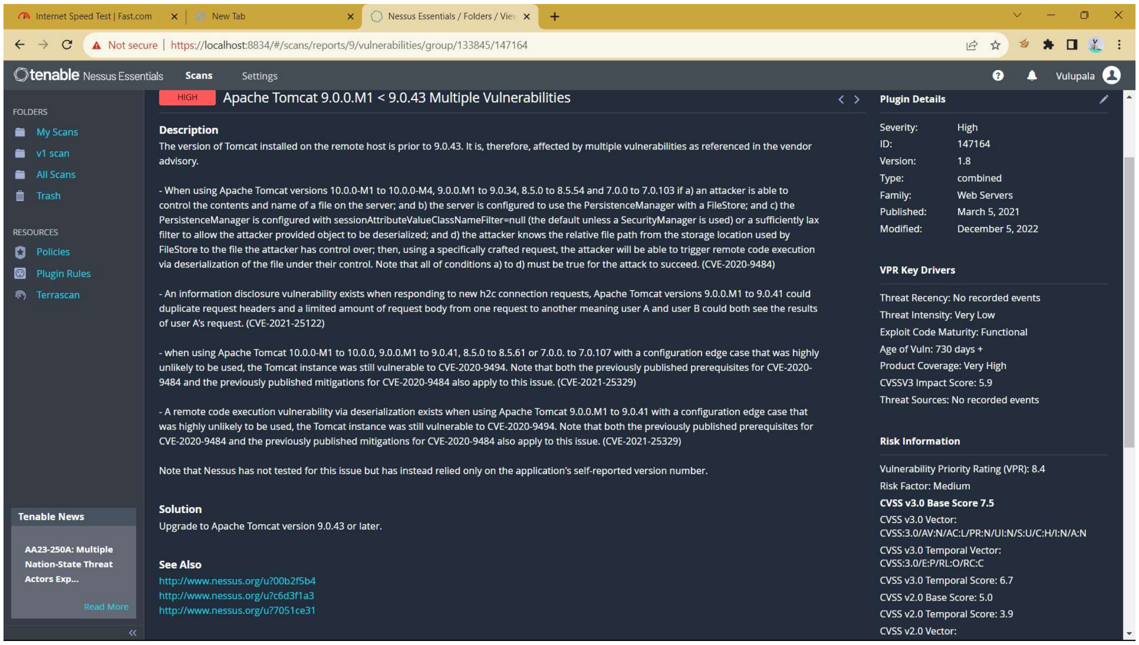
Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Base Score: 5.8

CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N


Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Folders / View
Not secure
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/133845/147164
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
AA23-250A: Multiple Nation-State Threat Actors Exp...
Read More
HIGH

HIGH Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 9.0.43. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor advisory.

- When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter=null (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed. (CVE-2020-9484)

- An information disclosure vulnerability exists when responding to new h2c connection requests, Apache Tomcat versions 9.0.0.M1 to 9.0.41 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request. (CVE-2021-25122)

- 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. (CVE-2021-25329)

- A remote code execution vulnerability via deserialization exists when using Apache Tomcat 9.0.0.M1 to 9.0.41 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. (CVE-2021-25329)

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 9.0.43 or later.

See Also

http://www.nessus.org/u?00b2f5b4
http://www.nessus.org/u?c6d3f1a3
http://www.nessus.org/u?7051ce31

Plugin Details

Severity:	High
ID:	147164
Version:	1.8
Type:	combined
Family:	Web Servers
Published:	March 5, 2021
Modified:	December 5, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 8.4

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

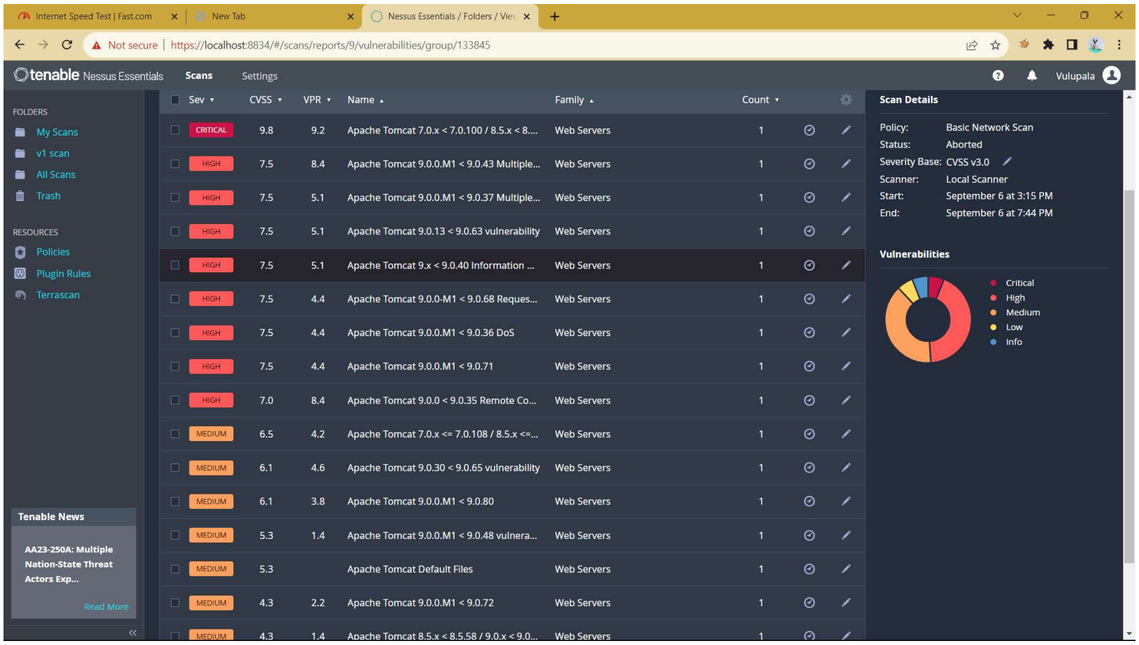
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:P/RL:O/RC:C

CVSS v3.0 Temporal Score: 6.7

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.9

CVSS v2.0 Vector:


Internet Speed Test | Fast.com
New Tab
Nessus Essentials / Folders / View
Not secure
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/133845
tenable Nessus Essentials
Scans
Settings
Vulupala
FOLDERS
My Scans
v1 scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
AA23-250A: Multiple Nation-State Threat Actors Exp...
Read More
Critical
High
Medium
Low
Info

□	Sev	CVSS	VPR	Name	Family	Count		
□	CRITICAL	9.8	9.2	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8....	Web Servers	1		
□	HIGH	7.5	8.4	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple...	Web Servers	1		
□	HIGH	7.5	5.1	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple...	Web Servers	1		
□	HIGH	7.5	5.1	Apache Tomcat 9.0.13 < 9.0.63 vulnerability	Web Servers	1		
□	HIGH	7.5	5.1	Apache Tomcat 9.x < 9.0.40 Information ...	Web Servers	1		
□	HIGH	7.5	4.4	Apache Tomcat 9.0.0-M1 < 9.0.68 Reques...	Web Servers	1		
□	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.36 DoS	Web Servers	1		
□	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.71	Web Servers	1		
□	HIGH	7.0	8.4	Apache Tomcat 9.0.0 < 9.0.35 Remote Co...	Web Servers	1		
□	MEDIUM	6.5	4.2	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <=...	Web Servers	1		
□	MEDIUM	6.1	4.6	Apache Tomcat 9.0.30 < 9.0.65 vulnerability	Web Servers	1		
□	MEDIUM	6.1	3.8	Apache Tomcat 9.0.0.M1 < 9.0.80	Web Servers	1		
□	MEDIUM	5.3	1.4	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnera...	Web Servers	1		
□	MEDIUM	5.3		Apache Tomcat Default Files	Web Servers	1		
□	MEDIUM	4.3	2.2	Apache Tomcat 9.0.0.M1 < 9.0.72	Web Servers	1		
□	MEDIUM	4.3	1.4	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0...	Web Servers	1		

Scan Details

Policy: Basic Network Scan
Status: Aborted
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 6 at 3:15 PM
End: September 6 at 7:44 PM

Vulnerabilities