System That Uses AI For Real-Time Data Classification, Leak Detection, And Prevention To Enhance Data Security.

Main Website: vtop2.vitap.ac.in

Practice Website: testphp.vulnweb.com

Vulnerabilities found in main website:

1. **133845 - Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities**

   CVE: CVE-2019-17569/ CVE-3030-2935/ CVE-2020-1938

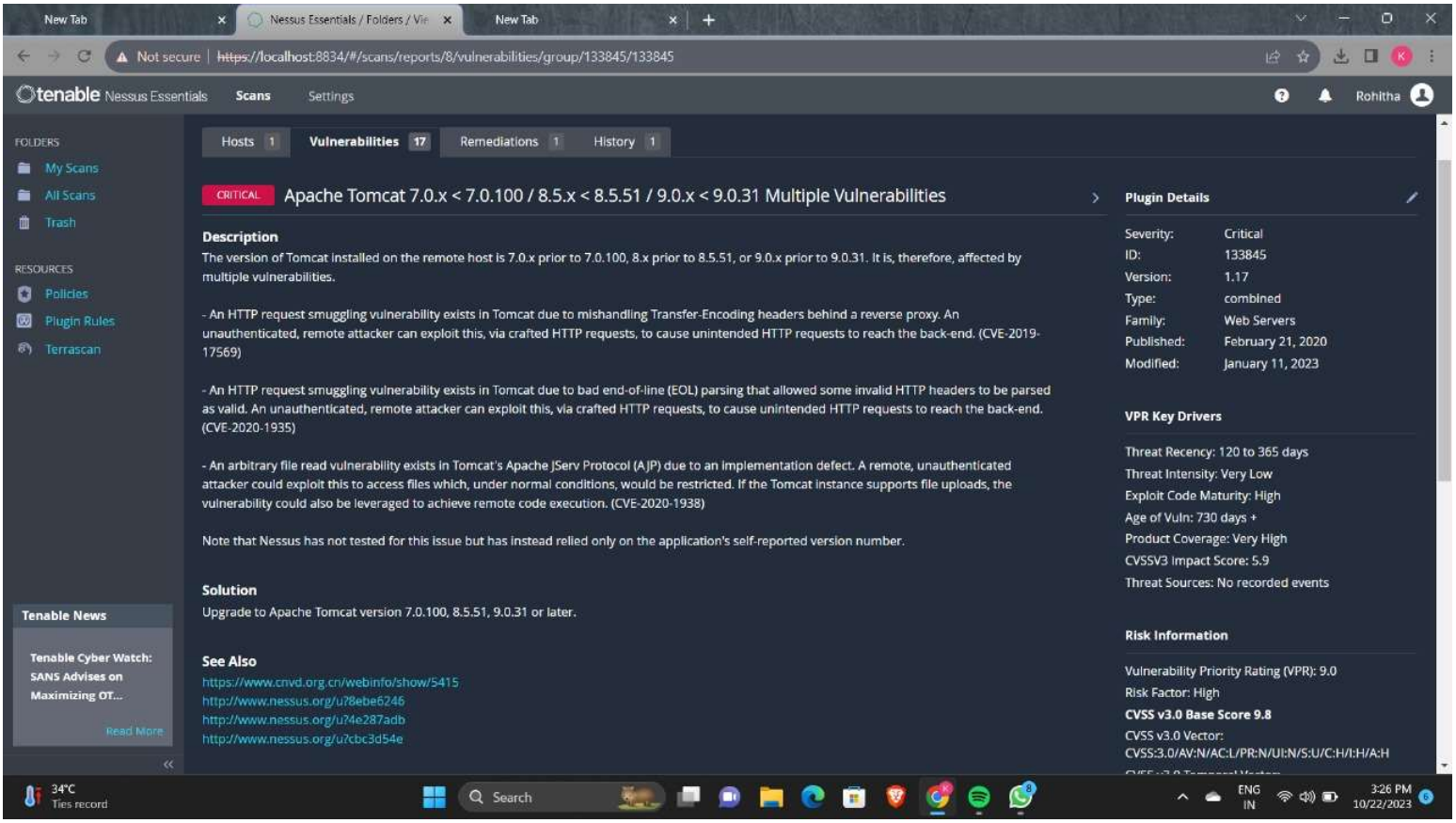
   Synopsis
   The remote Apache Tomcat server is affected by multiple vulnerabilities.

   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)



2. **111069 - Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilities**

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

CVE: CVE-2018-8014

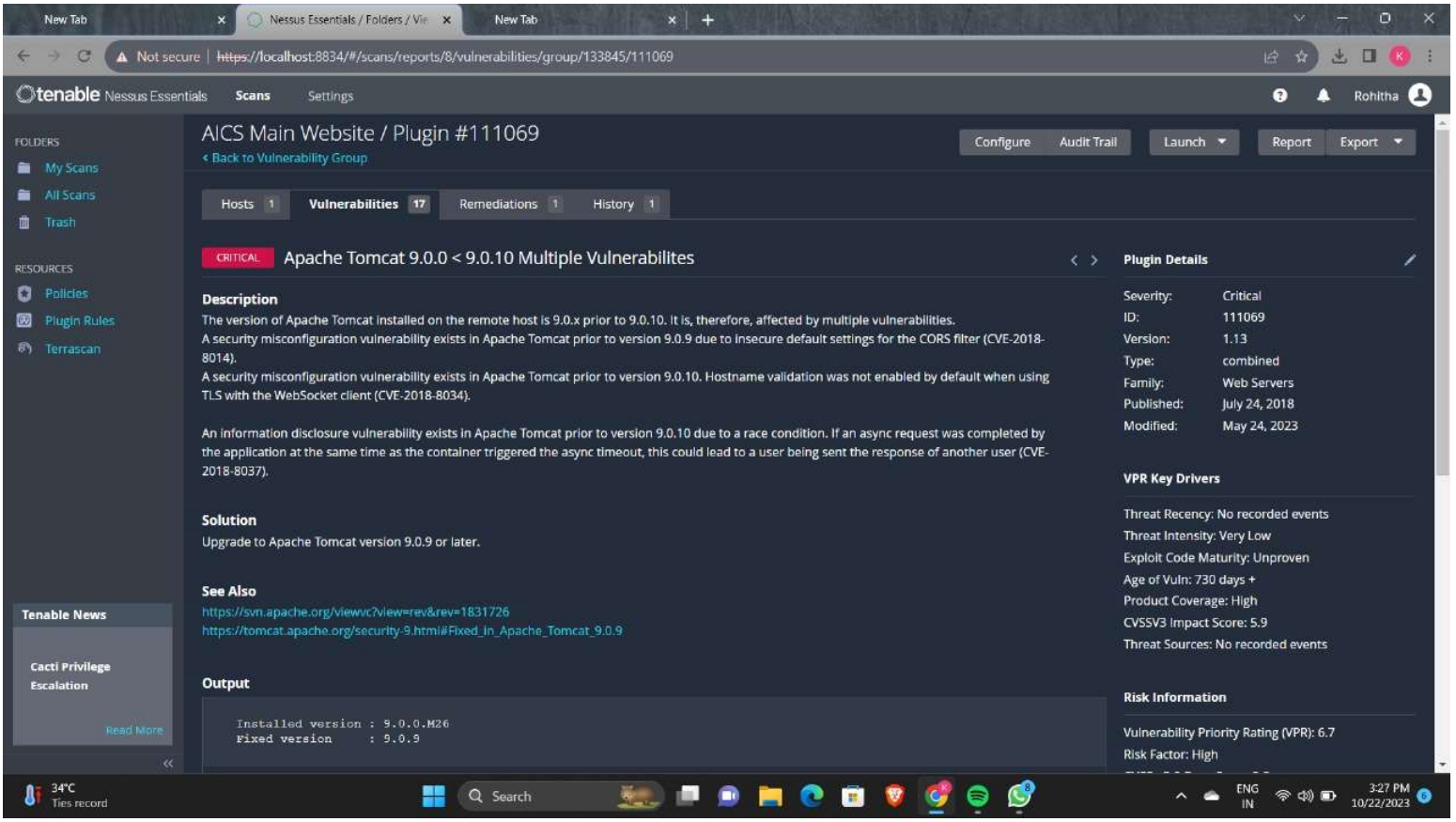
Description

The version of Apache Tomcat installed on the remote host is 9.0.x prior to 9.0.10. It is, therefore, affected by multiple vulnerabilities.

A security misconfiguration vulnerability exists in Apache Tomcat prior to version 9.0.9 due to insecure default settings for the CORS filter (CVE-2018-8014).

A security misconfiguration vulnerability exists in Apache Tomcat prior to version 9.0.10. Hostname validation was not enabled by default when using TLS with the WebSocket client (CVE-2018-8034).

An information disclosure vulnerability exists in Apache Tomcat prior to version 9.0.10 due to a race condition. If an async request was completed by the application at the same time as the container triggered the async timeout, this could lead to a user being sent the response of another user (CVE-2018-8037).



3. **161159 - Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability**

Synopsis

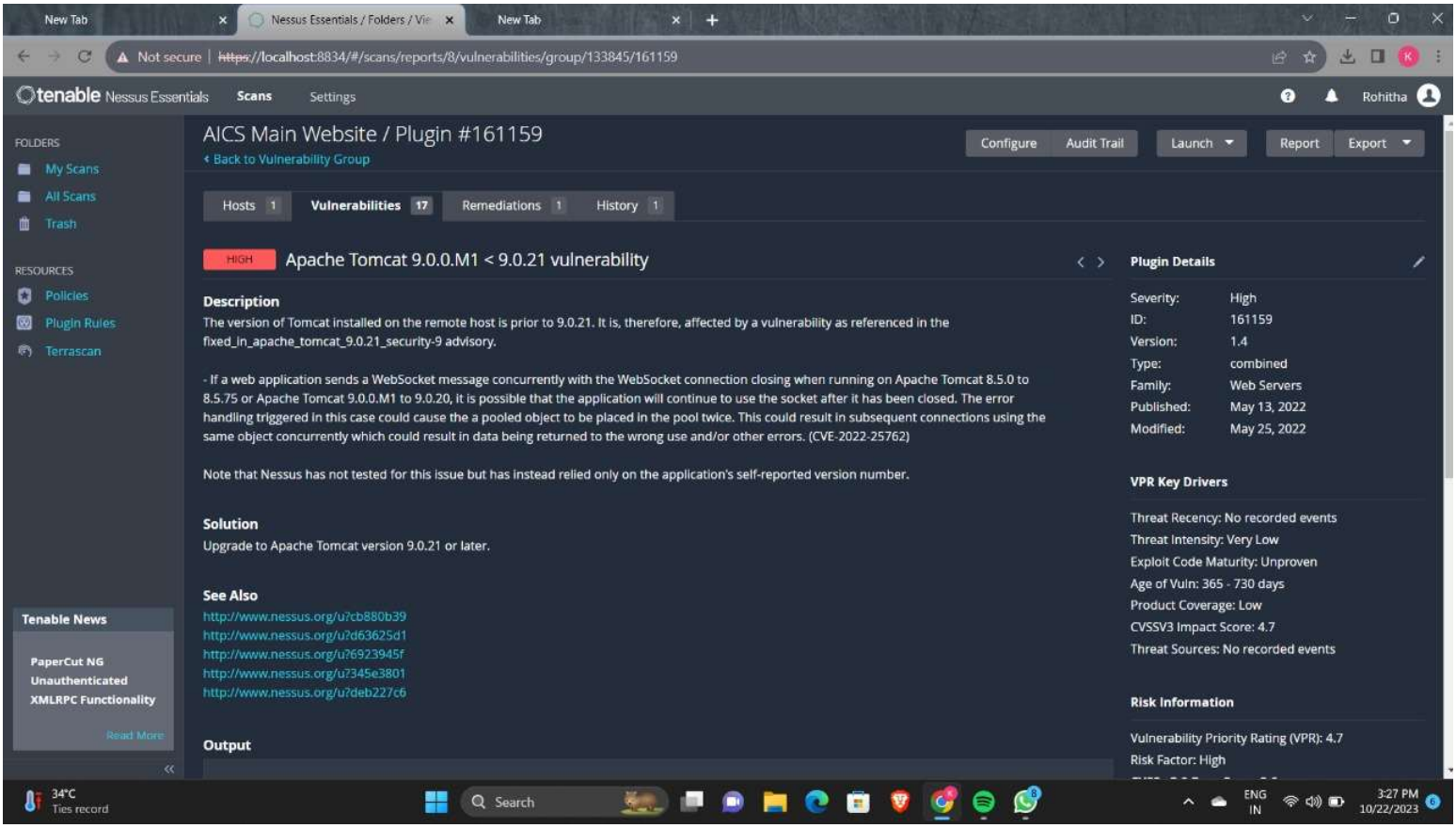
The remote Apache Tomcat server is affected by a vulnerability

CVE: CVE-2022-25762

Description

The version of Tomcat installed on the remote host is prior to 9.0.21. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.21_security-9 advisory.

- If a web application sends a WebSocket message concurrently with the WebSocket connection closing when running on Apache Tomcat 8.5.0 to 8.5.75 or Apache Tomcat 9.0.0.M1 to 9.0.20, it is possible that the application will continue to use the socket after it has been closed. The error handling triggered in this case could cause the a pooled object to be placed in the pool twice. This could result in subsequent connections using the same object concurrently which could result in data being returned to the wrong use and/or other errors. (CVE-2022-25762)



4. **122447 - Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability**

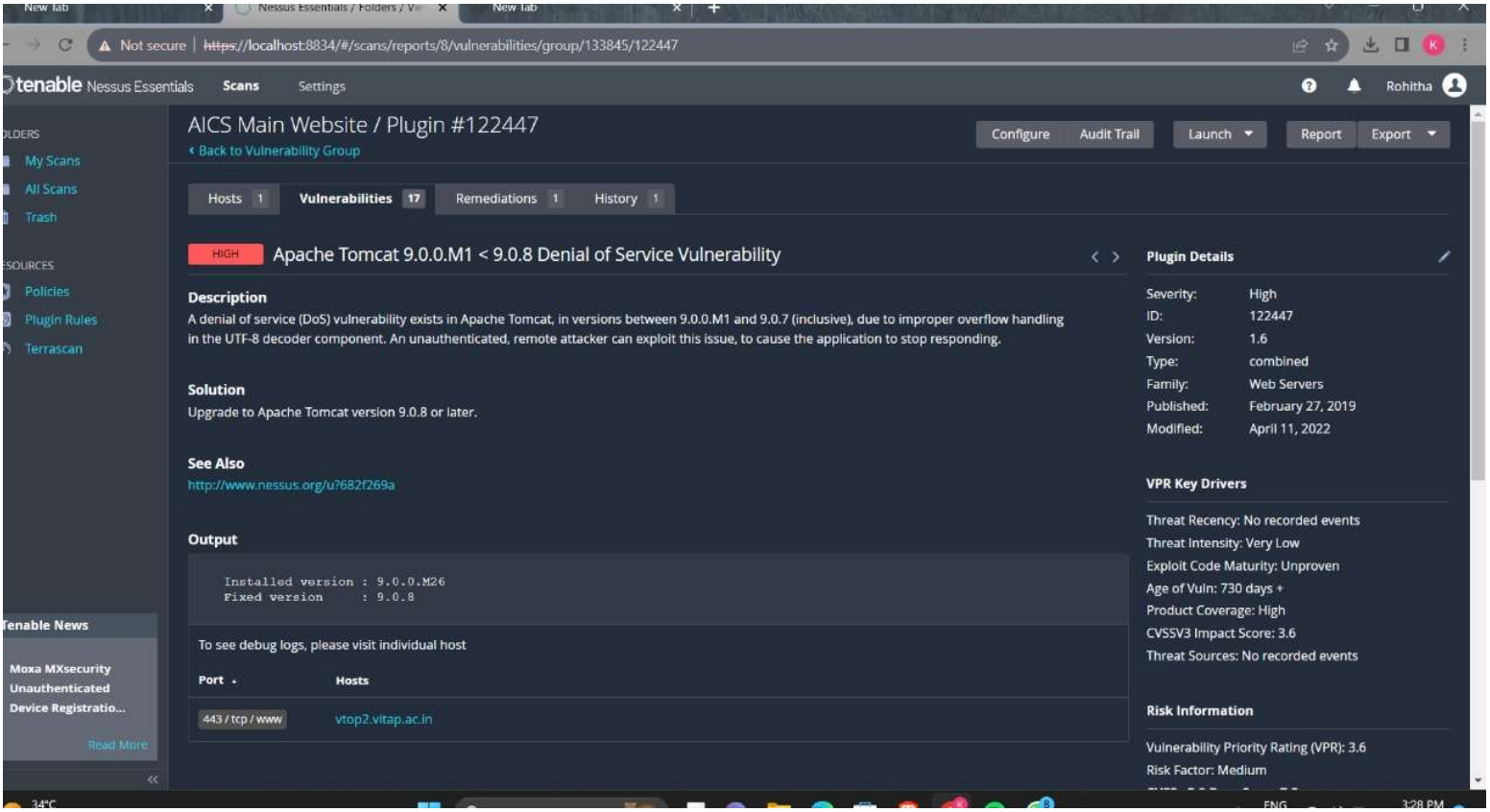
Synopsis

The remote Apache Tomcat server is affected by a denial of service vulnerability

CVE: CVE-2018-1336

Description

A denial of service (DoS) vulnerability exists in Apache Tomcat, in versions between 9.0.0.M1 and 9.0.7 (inclusive), due to improper overflow handling in the UTF-8 decoder component. An unauthenticated, remote attacker can exploit this issue, to cause the application to stop responding.



5. **136806 - Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution**

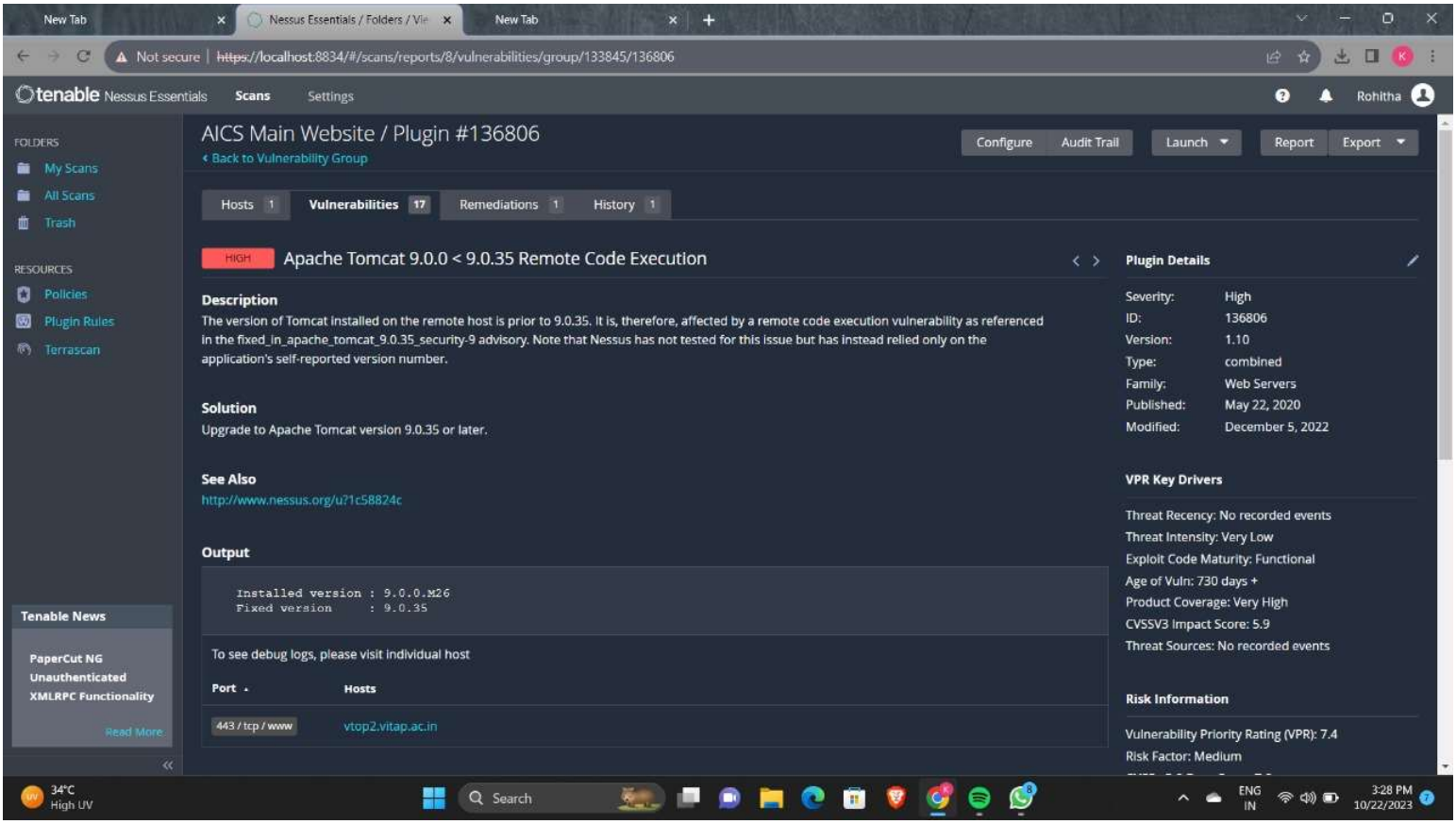
Synopsis

The remote Apache Tomcat server is affected by a remote code execution vulnerability

CVE: CVE-2020-9484

Description

The version of Tomcat installed on the remote host is prior to 9.0.35. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed_in_apache_tomcat_9.0.35_security-9 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.



6. 104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

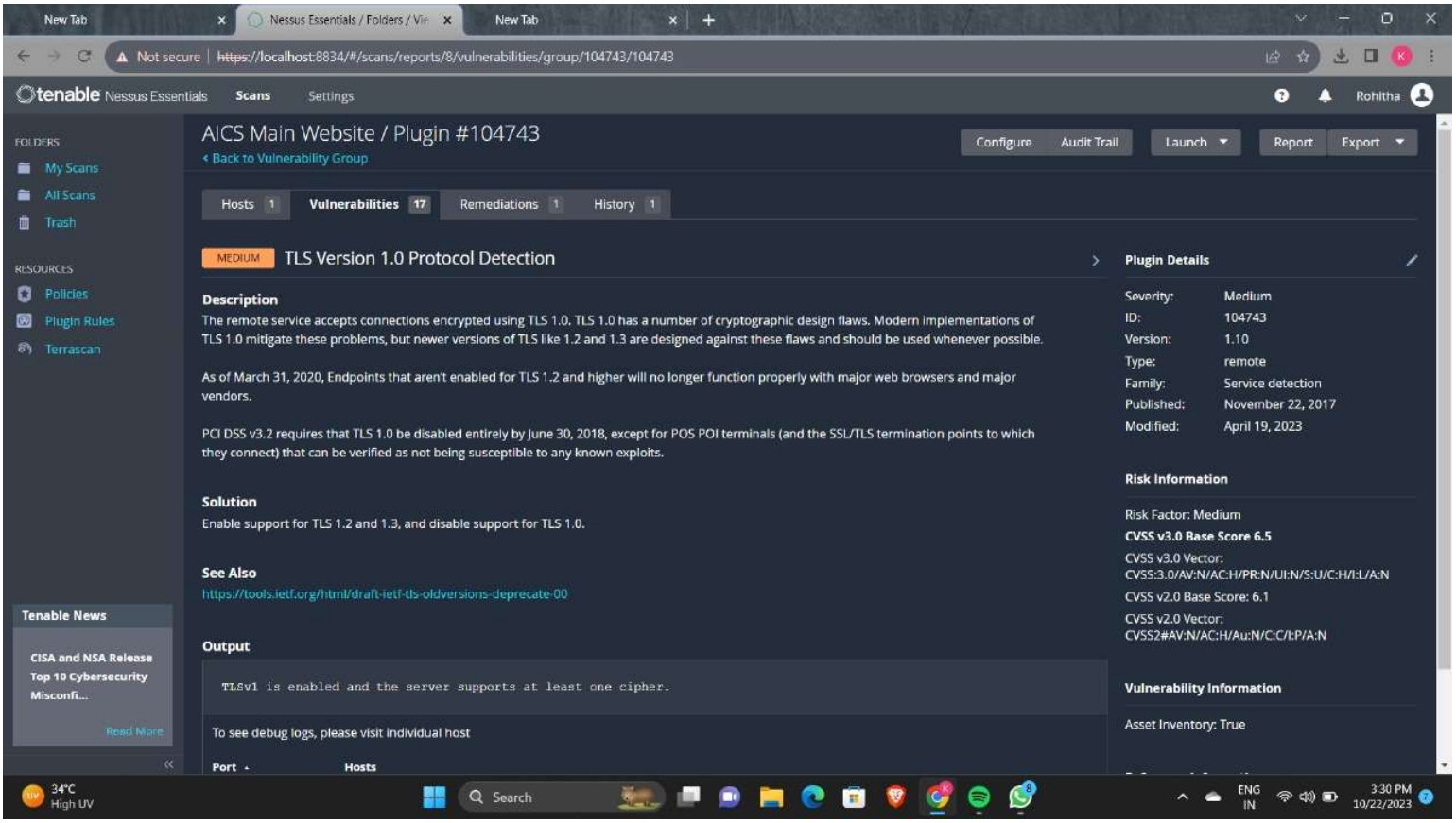
CWE: CWE-327

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.



7. 157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

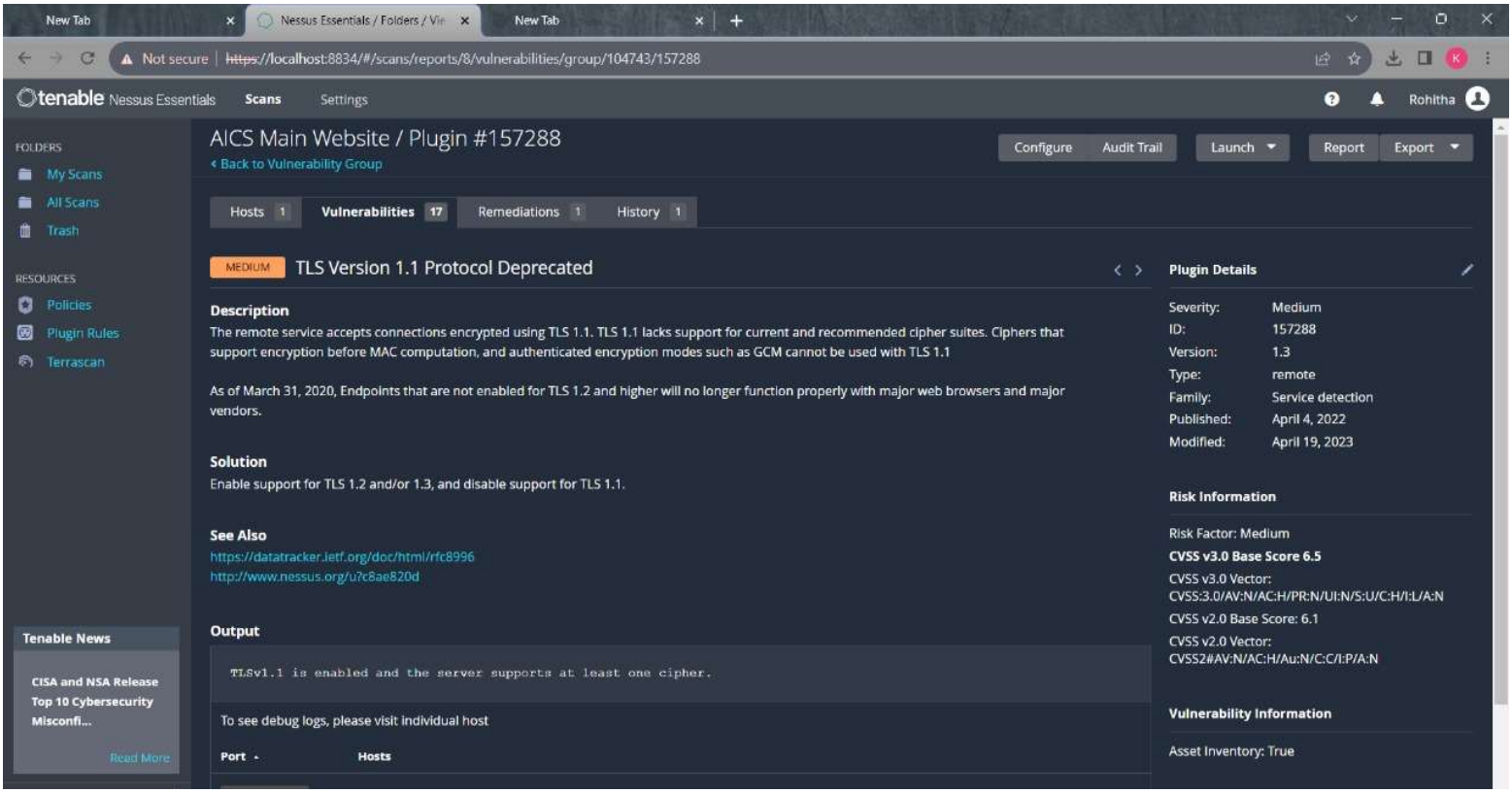
The remote service encrypts traffic using an older version of TLS.

CWE: CWE:327

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.


New Tab
Nessus Essentials / Folders / Vie
New Tab
Not secure | https://localhost:8834/#/scans/reports/8/vulnerabilities/group/104743/157288
tenable Nessus Essentials
Scans
Settings
Rohitha
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CISA and NSA Release Top 10 Cybersecurity Misconfi...
Read More
AICS Main Website / Plugin #157288
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 17
Remediations 1
History 1
MEDIUM
TLS Version 1.1 Protocol Deprecated
Description
The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
Solution
Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
See Also
https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d
Output
TLSv1.1 is enabled and the server supports at least one cipher.
To see debug logs, please visit individual host
Port
Hosts
Plugin Details
Severity: Medium
ID: 157288
Version: 1.3
Type: remote
Family: Service detection
Published: April 4, 2022
Modified: April 19, 2023
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N
Vulnerability Information
Asset Inventory: True