Secure Home Network Deployment

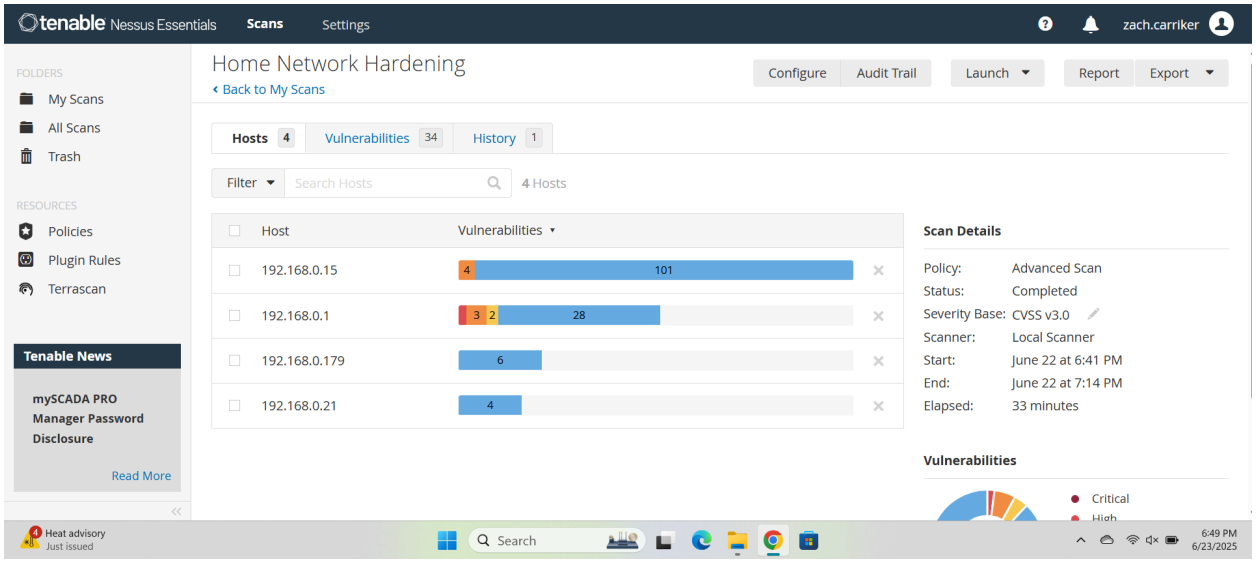
Initial Scan Setup:

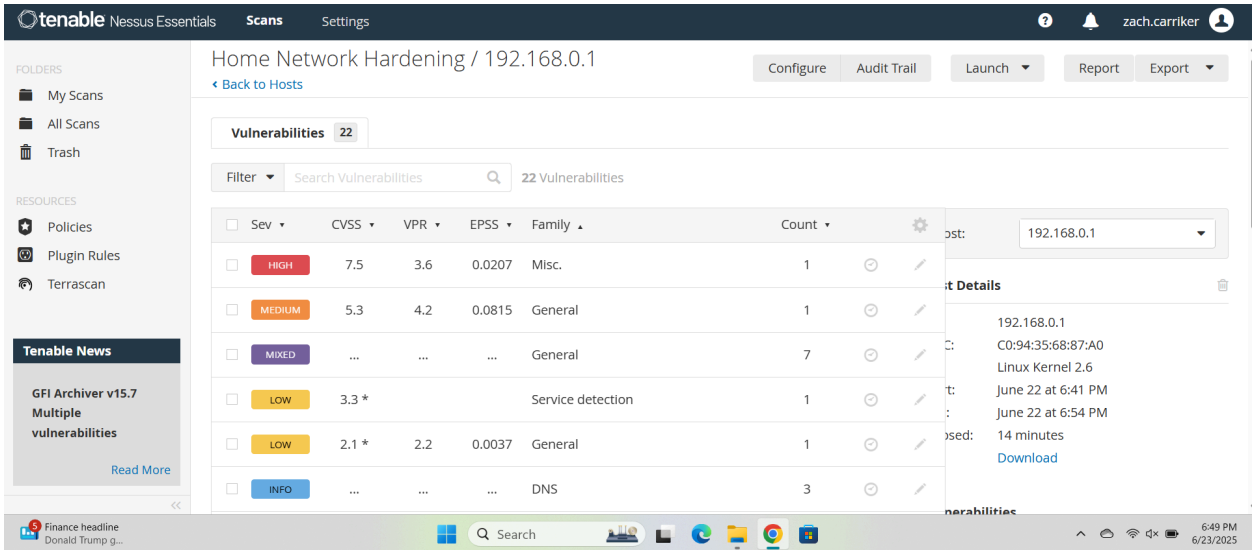
To begin the process of deploying a secure home network, I utilized Nessus Essentials to conduct an advanced vulnerability scan. This involved meticulously configuring a new scan after launching Nessus Essentials, precisely inputting the IP addresses of each target device to ensure comprehensive coverage. Adhering to best practices for a thorough security assessment, I applied the recommended configuration settings for an advanced scan profile, aiming to uncover a wide array of potential vulnerabilities that could compromise my home network's integrity. This scanning phase was a crucial step in identifying weaknesses before implementing remediation strategies to fortify my network's defenses.

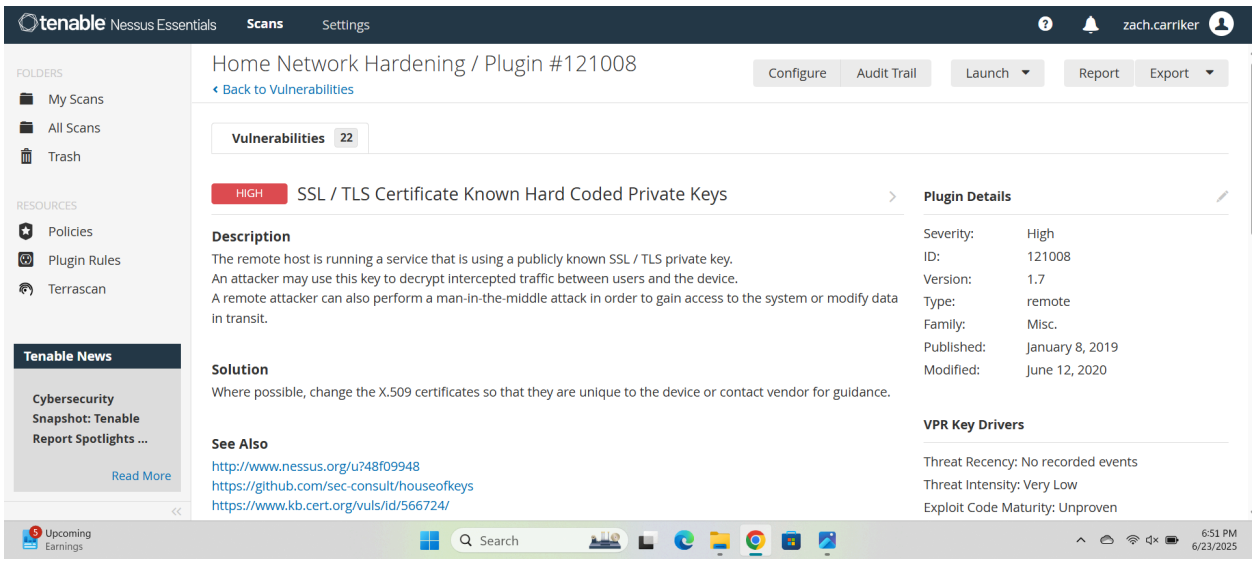
The devices targeted in these scans included:

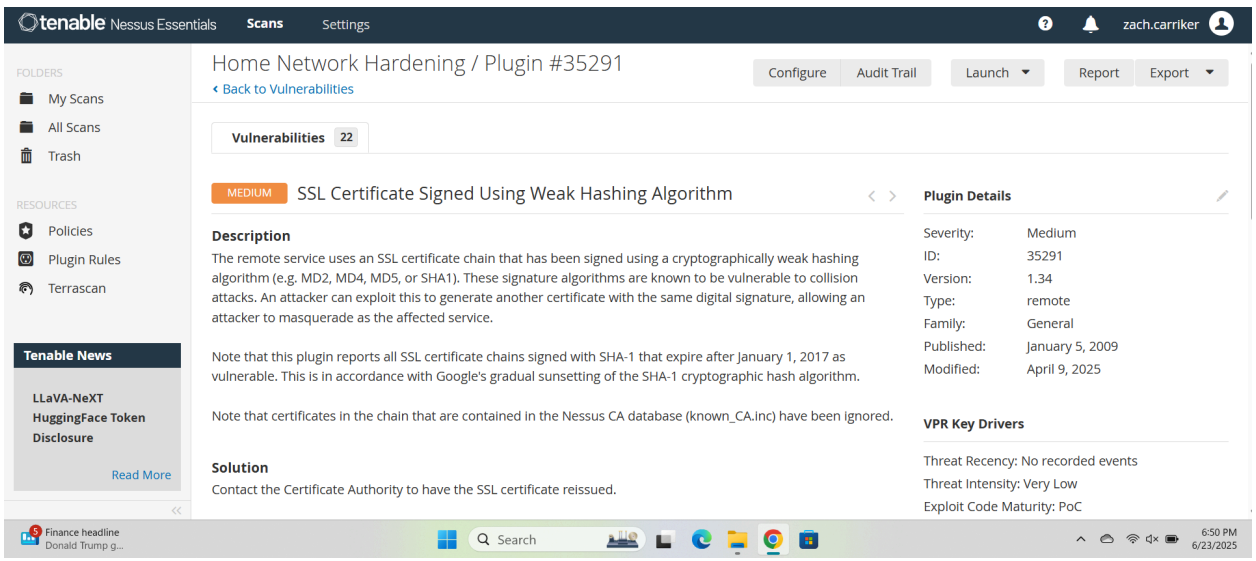
- Arris DG9450 (Original Gateway): 192.168.0.1 (Scanned in the initial baseline assessment before replacement)
- TP-Link Archer AX55 (Current Gateway): 192.168.0.1 (Scanned in subsequent re-assessments after replacement of the Arris gateway)
- Visio Smart TV 65 inch V series: 192.168.0.179
- Acer Aspire 5 Laptop: 192.168.0.15
- HP Google Chromebook: 192.168.0.21

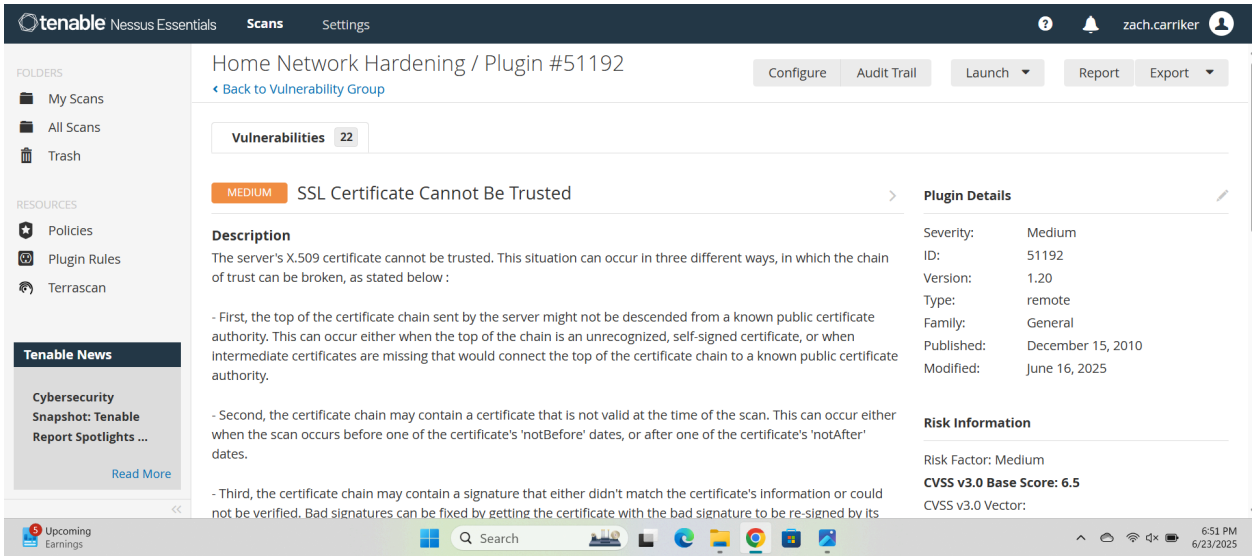
Initial Baseline Scan:

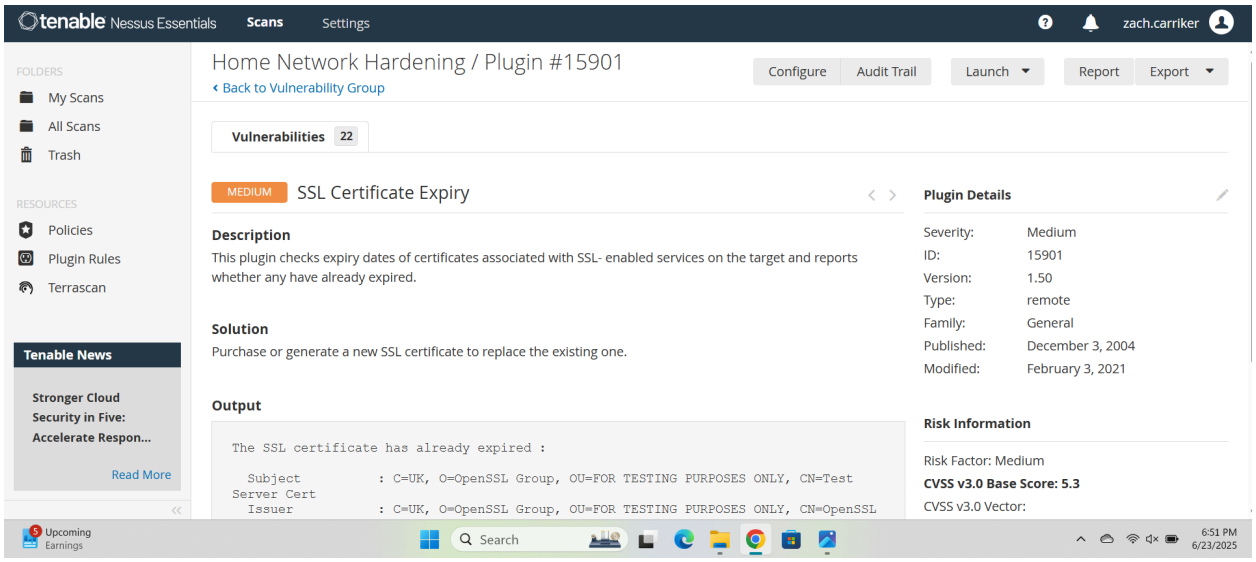


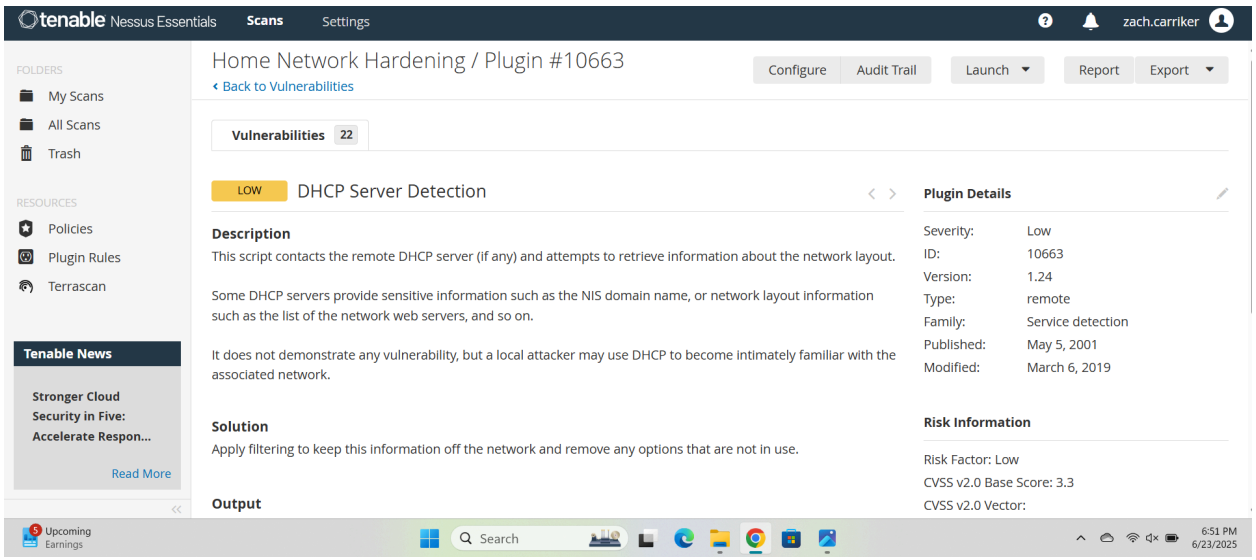

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
GFI Archiver v15.7 Multiple vulnerabilities
Read More
Home Network Hardening / 192.168.0.1
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
CVSS
VPR
EPSS
Family
Count
HIGH 7.5 3.6 0.0207 Misc. 1
MEDIUM 5.3 4.2 0.0815 General 1
MIXED ... ... General 7
LOW 3.3 * Service detection 1
LOW 2.1 * 2.2 0.0037 General 1
INFO ... ... DNS 3
192.168.0.1
Details
192.168.0.1
C0:94:35:68:87:A0
Linux Kernel 2.6
June 22 at 6:41 PM
June 22 at 6:54 PM
14 minutes
Download
Finance headline
Donald Trump g...
Search
6:49 PM
6/23/2025

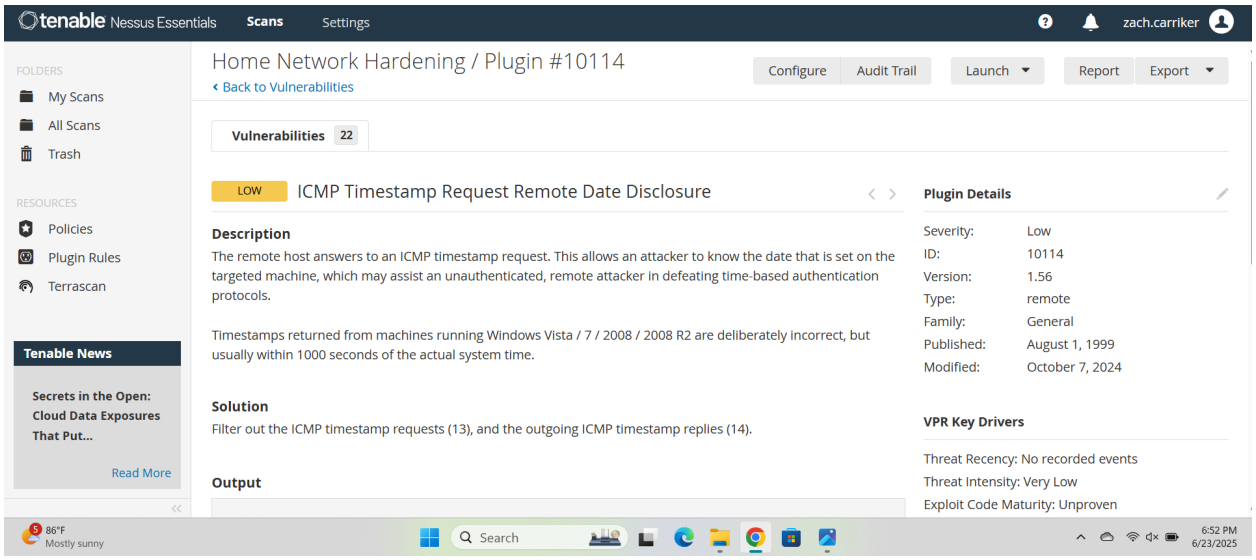

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Tenable Report Spotlights ...
Read More
Home Network Hardening / Plugin #121008
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
HIGH SSL / TLS Certificate Known Hard Coded Private Keys
Description
The remote host is running a service that is using a publicly known SSL / TLS private key.
An attacker may use this key to decrypt intercepted traffic between users and the device.
A remote attacker can also perform a man-in-the-middle attack in order to gain access to the system or modify data in transit.
Solution
Where possible, change the X.509 certificates so that they are unique to the device or contact vendor for guidance.
See Also
http://www.nessus.org/u?48f09948
https://github.com/sec-consult/houseofkeys
https://www.kb.cert.org/vuls/id/566724/
Plugin Details
Severity: High
ID: 121008
Version: 1.7
Type: remote
Family: Misc.
Published: January 8, 2019
Modified: June 12, 2020
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Upcoming Earnings
Search
6:51 PM
6/23/2025

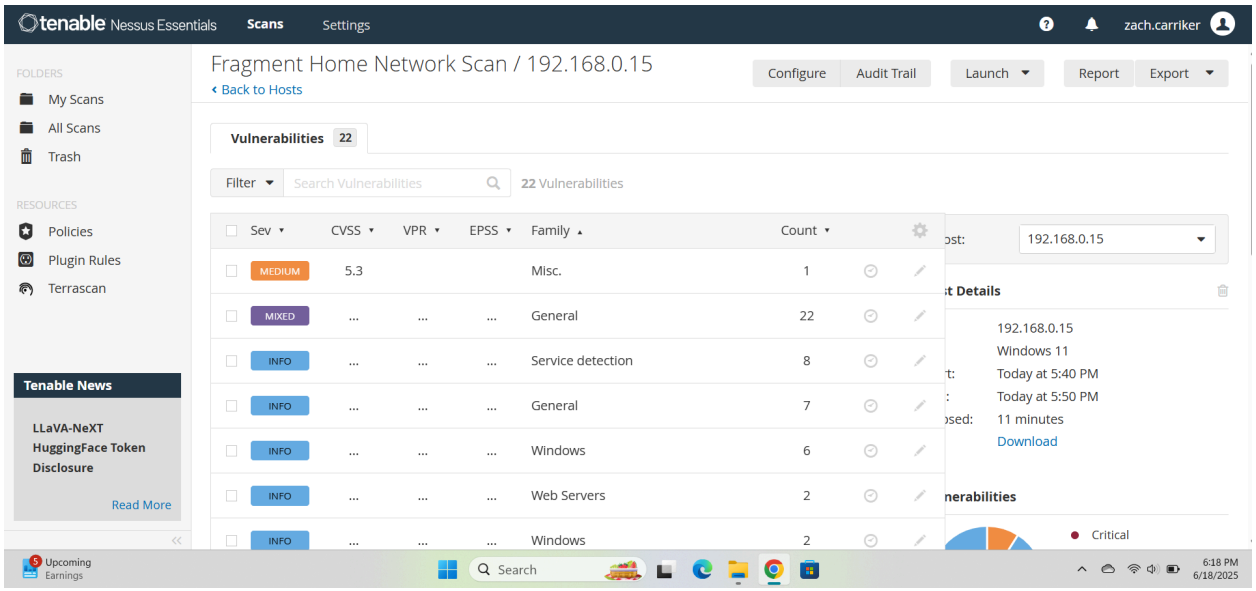

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
LLaVA-NeXT HuggingFace Token Disclosure
Read More
Home Network Hardening / Plugin #35291
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
MEDIUM SSL Certificate Signed Using Weak Hashing Algorithm
Description
The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.
Solution
Contact the Certificate Authority to have the SSL certificate reissued.
Plugin Details
Severity: Medium
ID: 35291
Version: 1.34
Type: remote
Family: General
Published: January 5, 2009
Modified: April 9, 2025
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Finance headline
Donald Trump g...
Search
6:50 PM
6/23/2025

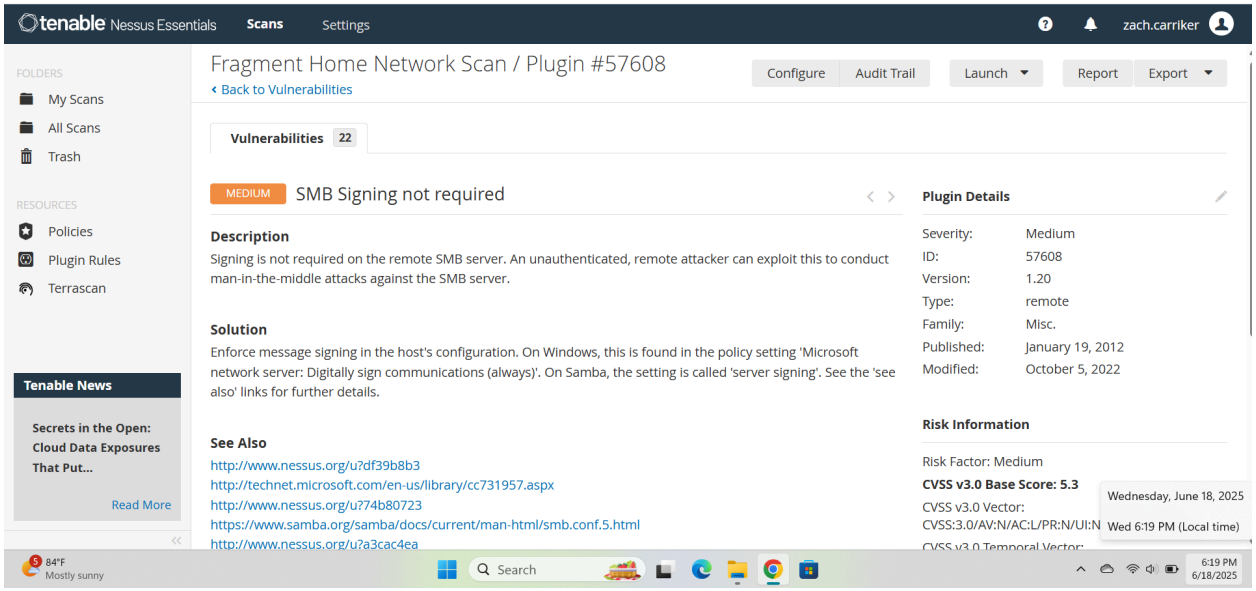

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Tenable Report Spotlights ...
Read More
Home Network Hardening / Plugin #51192
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
MEDIUM
SSL Certificate Cannot Be Trusted
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its
Plugin Details
Severity: Medium
ID: 51192
Version: 1.20
Type: remote
Family: General
Published: December 15, 2010
Modified: June 16, 2025
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:
Upcoming Earnings
Search
6:51 PM
6/23/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Stronger Cloud Security in Five: Accelerate Respon...
Read More
Home Network Hardening / Plugin #15901
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
MEDIUM
SSL Certificate Expiry
Description
This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.
Solution
Purchase or generate a new SSL certificate to replace the existing one.
Output
The SSL certificate has already expired :
Subject : C=UK, O=OpenSSL Group, OU=FOR TESTING PURPOSES ONLY, CN=Test Server Cert
Issuer : C=UK, O=OpenSSL Group, OU=FOR TESTING PURPOSES ONLY, CN=OpenSSL
Plugin Details
Severity: Medium
ID: 15901
Version: 1.50
Type: remote
Family: General
Published: December 3, 2004
Modified: February 3, 2021
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector:
Upcoming Earnings
Search
6:51 PM
6/23/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Stronger Cloud Security in Five: Accelerate Respon...
Read More
Home Network Hardening / Plugin #10663
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
LOW
DHCP Server Detection
Description
This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.
Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.
It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.
Solution
Apply filtering to keep this information off the network and remove any options that are not in use.
Output
Plugin Details
Severity: Low
ID: 10663
Version: 1.24
Type: remote
Family: Service detection
Published: May 5, 2001
Modified: March 6, 2019
Risk Information
Risk Factor: Low
CVSS v2.0 Base Score: 3.3
CVSS v2.0 Vector:
Upcoming Earnings
Search
6:51 PM
6/23/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Secrets in the Open: Cloud Data Exposures That Put...
Read More
Home Network Hardening / Plugin #10114
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 22
LOW
ICMP Timestamp Request Remote Date Disclosure
Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Output
Plugin Details
Severity: Low
ID: 10114
Version: 1.56
Type: remote
Family: General
Published: August 1, 1999
Modified: October 7, 2024
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
86°F
Mostly sunny
Search
6:52 PM
6/23/2025





Initial Vulnerability Scan Results:

A vulnerability scan of the home network identified a total of 34 vulnerabilities across four hosts.

Router Vulnerabilities

The router (192.168.0.1, *referring to the original ISP-provided router before replacement*) displayed 28 vulnerabilities, with one categorized as high severity and two as medium. The high-severity vulnerability on the router is an SSL/TLS certificate with a known hard-coded private key, which could allow a remote attacker to decrypt intercepted traffic or perform man-in-the-middle attacks. Additional medium-severity vulnerabilities on the router include an SSL certificate signed using a weak hashing algorithm (such as MD5, MD2, MD4, or SHA1), an

expired SSL certificate, and an SSL certificate that cannot be trusted due to an unrecognized, self-signed, or improperly chained certificate. Low-severity findings on the router include DHCP server detection and ICMP Timestamp Request Remote Date Disclosure, which could reveal network layout information or assist attackers in defeating time-based authentication.

Laptop Vulnerabilities

The laptop (192.168.0.15) exhibited 101 vulnerabilities, with a significant number being informational but also including one medium-severity vulnerability related to SMB signing not being required. This absence of SMB signing could allow an unauthenticated remote attacker to conduct man-in-the-middle attacks against the SMB server. Overall, the scan highlights critical security weaknesses, particularly concerning the router's SSL/TLS configuration, which could lead to severe compromise of network communications and data integrity.

Remediation:

SSL Certificate Warnings

My vulnerability scan indicates warnings such as "SSL Self-Signed Certificate" and "SSL Certificate Cannot Be Trusted" across all my networked devices following the system upgrade. This is an anticipated and perfectly acceptable characteristic of a secure home network setup. By replacing the ISP's modem/router combo with my TP-Link AX55 and enabling HTTPS for local administrative access, I successfully remediated critical previous issues, including a high-severity vulnerability related to SSL/TLS certificates with known hard-coded private keys, as well as medium-severity warnings for certificates signed using weak hashing algorithms and expired certificates. The current "Self-Signed Certificate" and "Certificate Cannot Be Trusted" warnings are now the expected behavior for my private home network where obtaining a certificate from a public Certificate Authority is unnecessary and impractical. Nessus flags these because it cannot validate them against a trusted public CA chain, which is precisely how self-signed certificates function. The uniform appearance of these warnings across my devices simply confirms their connection to and interaction with the router's secure local interface. A comprehensive report detailing these configuration changes can be found in the attached Secure Home Network Deployment Report.

Host-Level Security Hardening on Acer Aspire 5

Significant host-level security hardening measures were implemented on the Acer Aspire 5 laptop, running Windows 11 Home. A key step involved enforcing cryptographic signing for Server Message Block (SMB) traffic, which was a previously identified vulnerability that could have allowed man-in-the-middle attacks. This was achieved by directly editing system registry keys, setting `RequireSecuritySignature` and `EnableSecuritySignature` to '1' under both the `LanmanServer` and `LanmanWorkstation` parameters, with PowerShell verification

confirming successful enforcement. Furthermore, to bolster protection for Remote Desktop Configuration (RDC), and recognizing that `gpedit.msc` is not available on Windows Home, I utilized **Policy Plus** to apply additional security policies. These policies were instrumental in disabling or restricting Remote Desktop access and enforcing stricter RDC authentication settings, thereby significantly reducing the system's exposure to unauthorized remote login attempts.

SSL Medium Strength Cipher Suites on Smart TV

The "SSL Medium Strength Cipher Suites Supported (SWEET32)" vulnerability identified on my Smart TV was notably **not detected in the initial vulnerability scan, becoming apparent only in the subsequent re-scan**, underscoring the critical importance of conducting post-remediation scans to fully verify the effectiveness of security measures and uncover previously missed issues. Despite efforts to update the TV's firmware, it was found to be currently up-to-date, indicating that the manufacturer has not released a patch to address this specific cryptographic weakness. Furthermore, the Smart TV's interface offers no granular control to reconfigure or disable these medium-strength cipher suites. Given these technical limitations and the inability to directly remediate the issue, the strategic decision has been made to isolate the Smart TV. It will be moved to an IoT (Internet of Things) Wi-Fi segment of the network, effectively segmenting it from other critical devices and sensitive data, thereby preventing this inherent weakness from impacting the overall security posture of the home network.

ICMP Timestamp Request Remote Date Disclosure

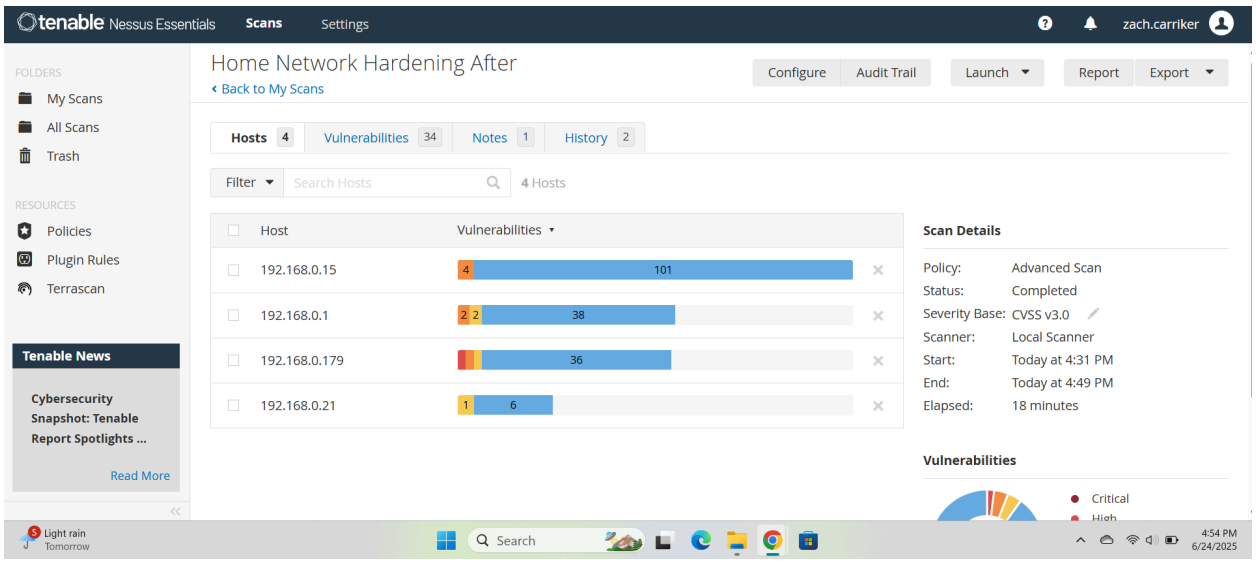
Despite diligently configuring the TP-Link Archer AX55 router to disable WAN (Internet-side) ping responses, the "ICMP Timestamp Request Remote Date Disclosure" vulnerability continues to appear across all scanned devices. This persistent detection is occurring primarily due to ICMP timestamp responses originating from the LAN (Local Area Network) interfaces of the devices themselves, as well as the router's deliberate response to LAN pings for diagnostic purposes. While ideally, all devices would filter these specific ICMP types (13 and 14), configuring each individual device to block these informational responses is a more involved process. For the immediate future, efforts to block this at the individual device level will be deferred, recognizing the low severity of this informational disclosure in a contained home network environment, especially with WAN-side protections in place.

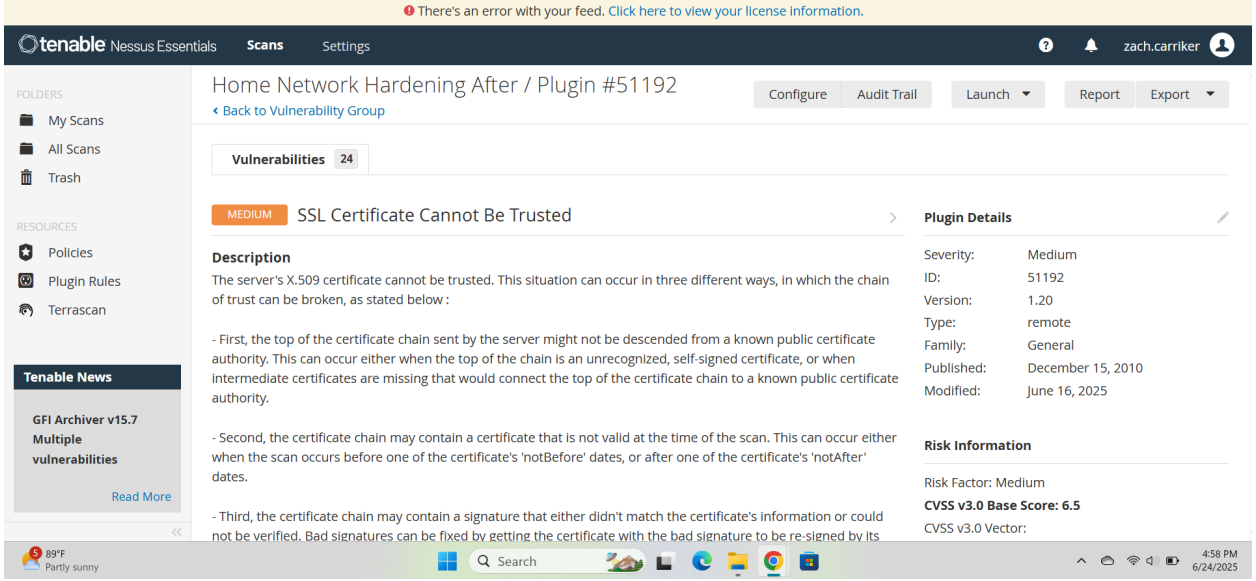
DHCP Server Detection

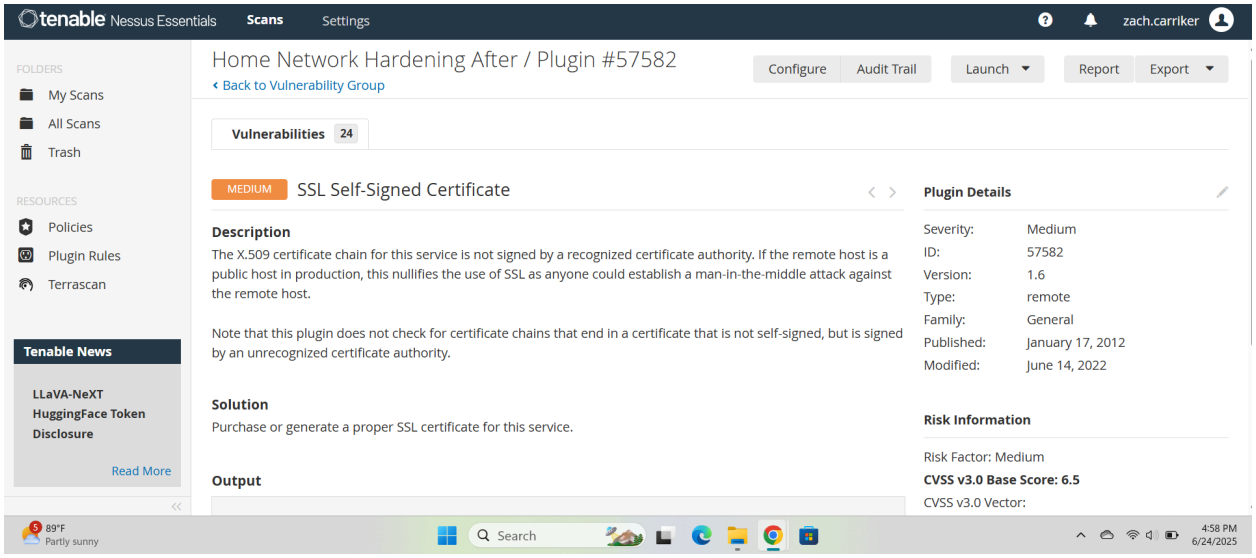
The "DHCP Server Detection" finding is a low-severity, informational alert from Nessus. It simply indicates the presence of a Dynamic Host Configuration Protocol (DHCP) server on the network, which is an essential service for automatically assigning IP addresses to connected devices and enabling network functionality. While Nessus suggests filtering out unnecessary network information, typical consumer-grade routers like the TP-Link AX55 offer limited advanced configuration options to suppress or hide the DHCP server's presence without disrupting normal

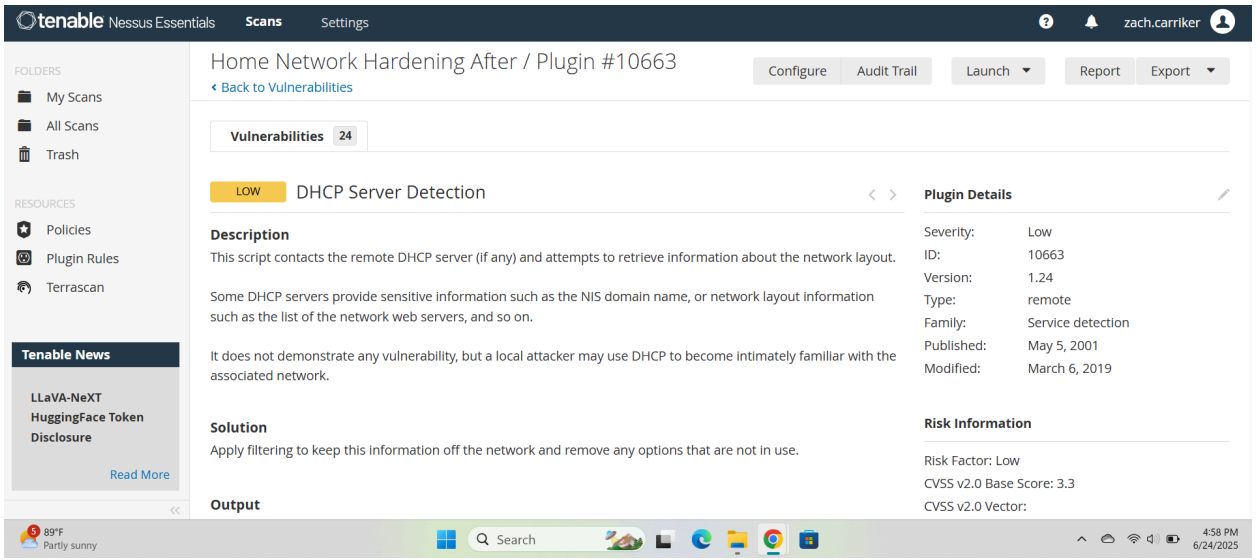
network operations. For a home network, the convenience and necessity of a functional DHCP server usually outweigh the minimal informational risk associated with this finding, which is more of an operational characteristic than a direct security vulnerability.

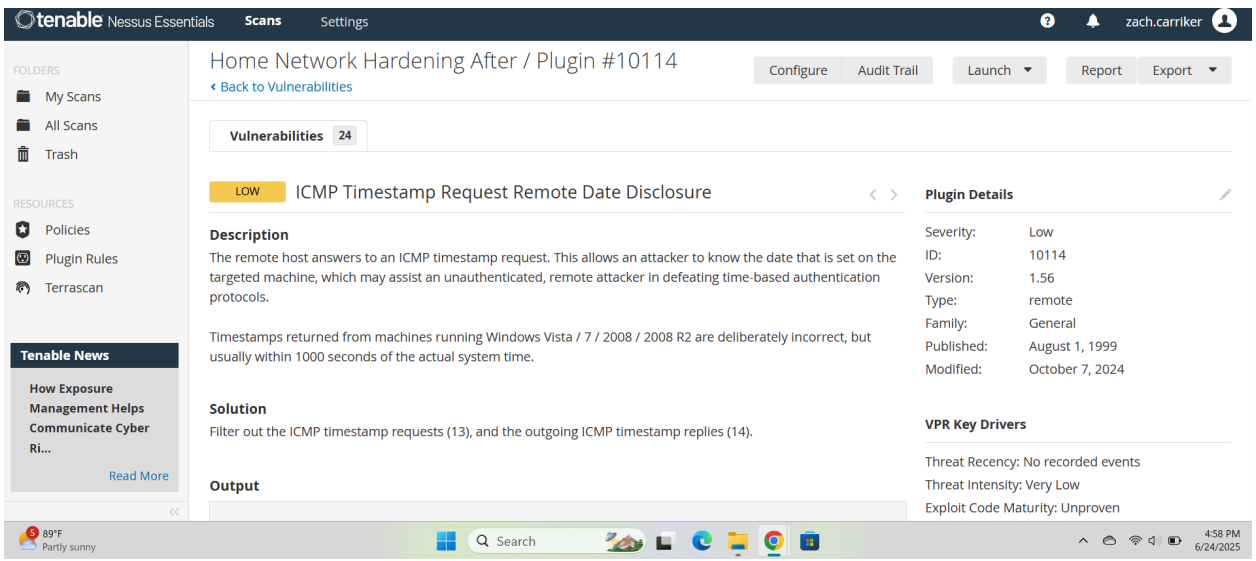
Subsequent Scan:

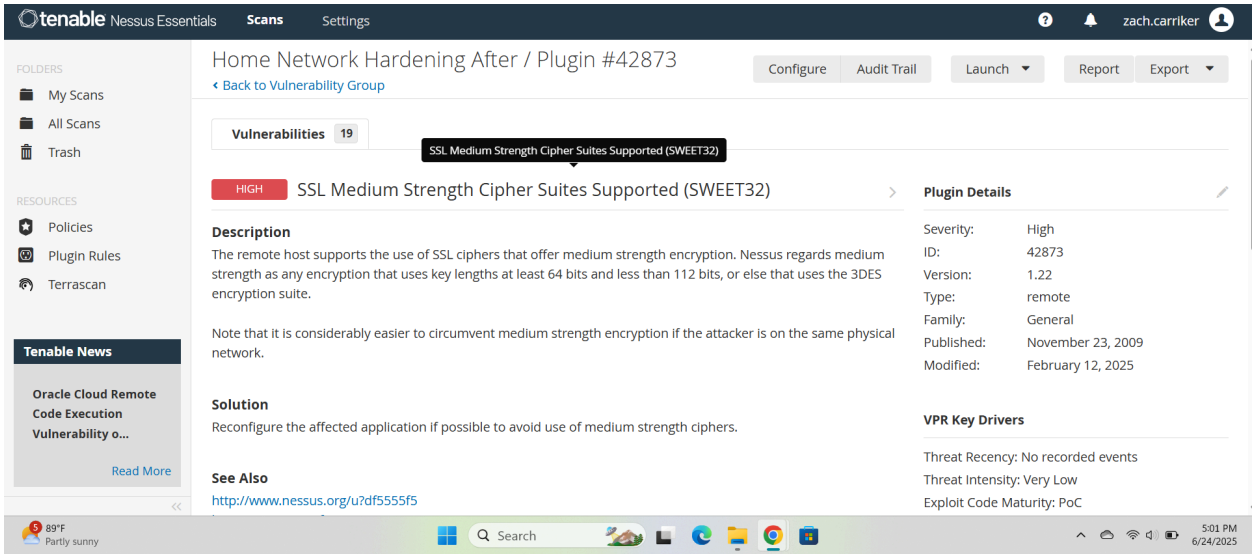


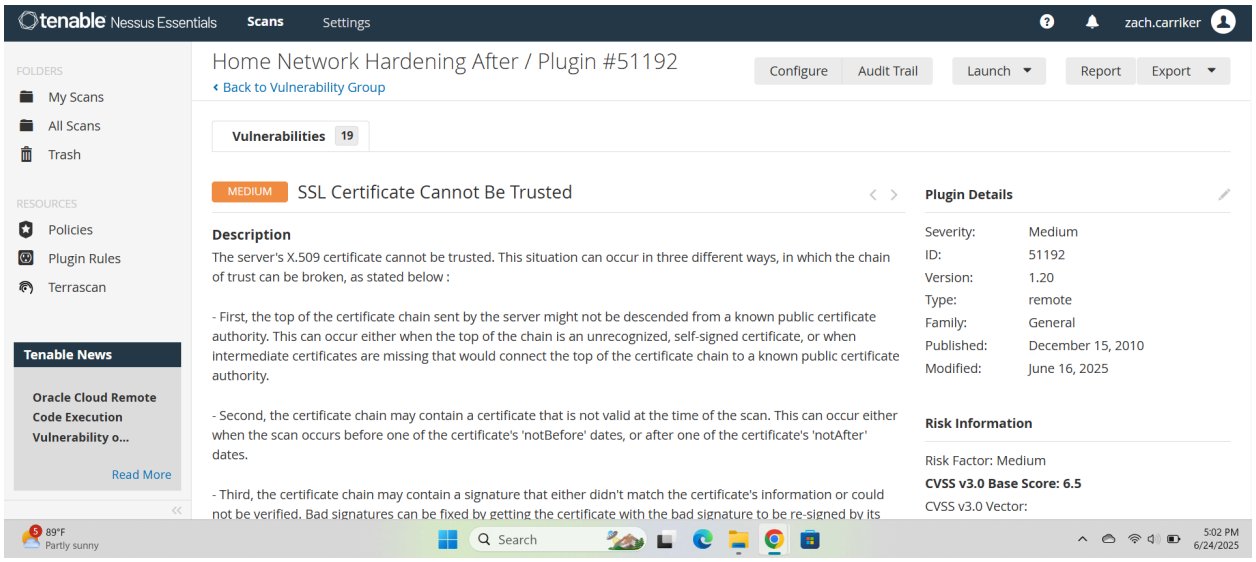


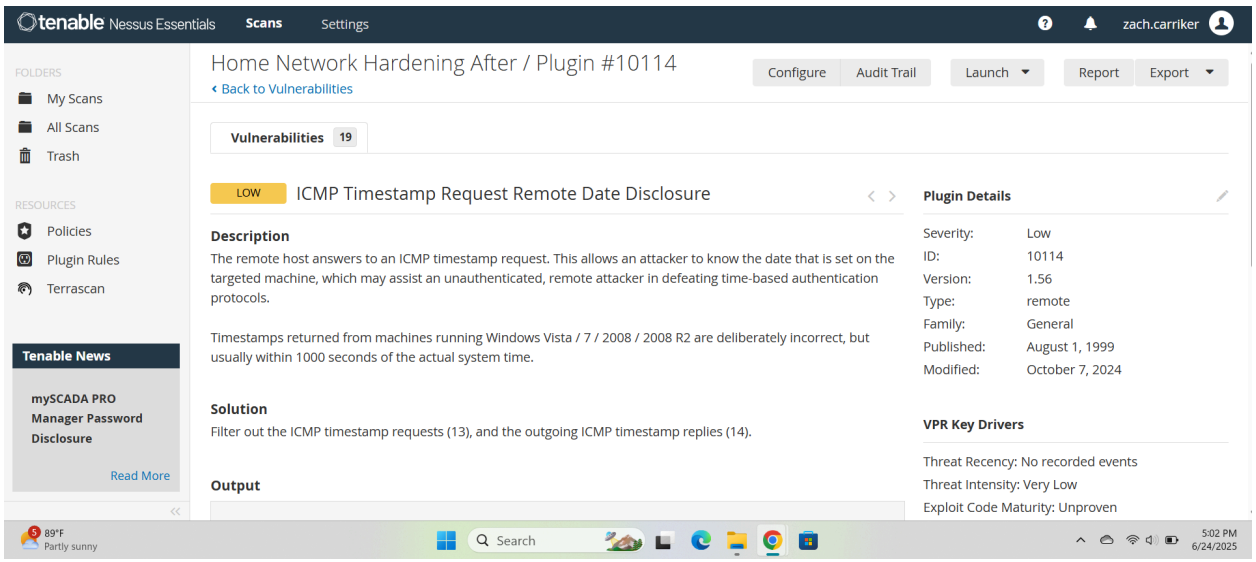

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
LLaVA-NeXT HuggingFace Token Disclosure
Read More
Home Network Hardening After / Plugin #57582
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 24
MEDIUM
SSL Self-Signed Certificate
Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.
Solution
Purchase or generate a proper SSL certificate for this service.
Output
Plugin Details
Severity: Medium
ID: 57582
Version: 1.6
Type: remote
Family: General
Published: January 17, 2012
Modified: June 14, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:
89°F Partly sunny
Search
4:58 PM 6/24/2025

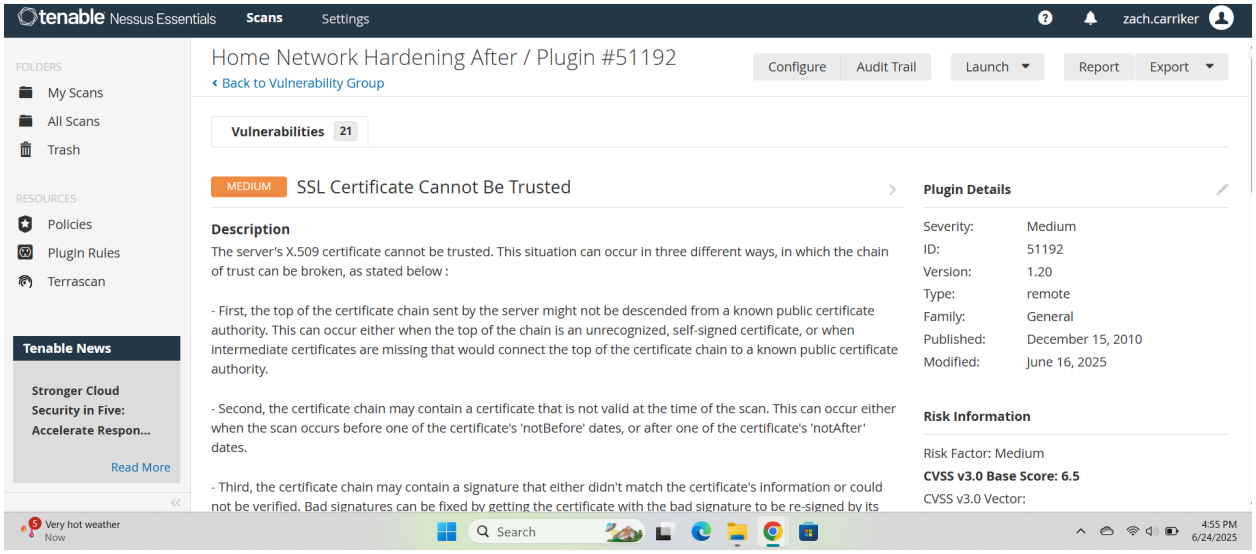

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
LLaVA-NeXT HuggingFace Token Disclosure
Read More
Home Network Hardening After / Plugin #10663
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 24
LOW
DHCP Server Detection
Description
This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.
Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.
It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.
Solution
Apply filtering to keep this information off the network and remove any options that are not in use.
Output
Plugin Details
Severity: Low
ID: 10663
Version: 1.24
Type: remote
Family: Service detection
Published: May 5, 2001
Modified: March 6, 2019
Risk Information
Risk Factor: Low
CVSS v2.0 Base Score: 3.3
CVSS v2.0 Vector:
89°F Partly sunny
Search
4:58 PM 6/24/2025

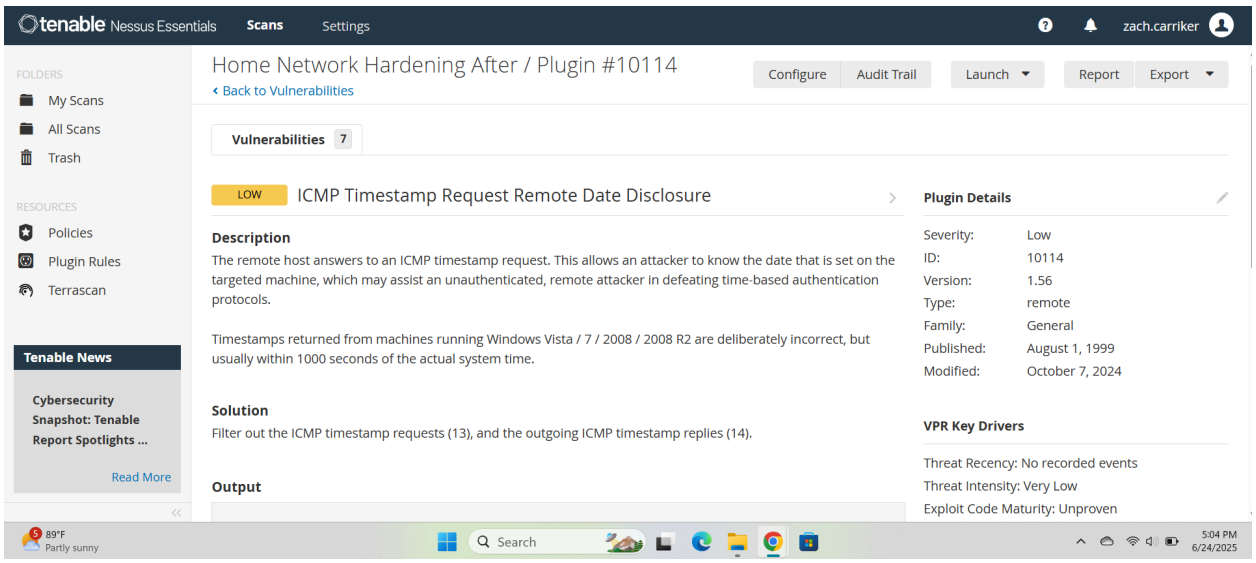

tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
How Exposure Management Helps Communicate Cyber Ri...
Read More
Home Network Hardening After / Plugin #10114
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 24
LOW
ICMP Timestamp Request Remote Date Disclosure
Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Output
Plugin Details
Severity: Low
ID: 10114
Version: 1.56
Type: remote
Family: General
Published: August 1, 1999
Modified: October 7, 2024
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
89°F Partly sunny
Search
4:58 PM 6/24/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle Cloud Remote Code Execution Vulnerability o...
Read More
Home Network Hardening After / Plugin #42873
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 19
SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH
SSL Medium Strength Cipher Suites Supported (SWEET32)
Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
Solution
Reconfigure the affected application if possible to avoid use of medium strength ciphers.
See Also
http://www.nessus.org/u?df5555f5
Plugin Details
Severity: High
ID: 42873
Version: 1.22
Type: remote
Family: General
Published: November 23, 2009
Modified: February 12, 2025
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
89°F
Partly sunny
Search
5:01 PM
6/24/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle Cloud Remote Code Execution Vulnerability o...
Read More
Home Network Hardening After / Plugin #51192
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 19
MEDIUM
SSL Certificate Cannot Be Trusted
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its
Plugin Details
Severity: Medium
ID: 51192
Version: 1.20
Type: remote
Family: General
Published: December 15, 2010
Modified: June 16, 2025
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:
89°F
Partly sunny
Search
5:02 PM
6/24/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
mySCADA PRO Manager Password Disclosure
Read More
Home Network Hardening After / Plugin #10114
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 19
LOW
ICMP Timestamp Request Remote Date Disclosure
Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Output
Plugin Details
Severity: Low
ID: 10114
Version: 1.56
Type: remote
Family: General
Published: August 1, 1999
Modified: October 7, 2024
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
89°F
Partly sunny
Search
5:02 PM
6/24/2025





Conclusion:

In conclusion, this project successfully addressed critical security vulnerabilities and significantly enhanced the overall security posture of the home network. The initial baseline scan revealed concerning high and medium-severity vulnerabilities, particularly related to the ISP-provided router's SSL/TLS configuration and the laptop's SMB signing. Through strategic device replacement, meticulous configuration, and host-level hardening using tools like Policy Plus, these major risks were effectively mitigated. While certain informational findings, such as self-signed SSL certificates, ICMP timestamp disclosure, and DHCP server detection, remain present, they are understood to be either expected behavior for a private network or low-severity characteristics with established acceptable risks. The implementation of robust security measures, including HTTPS for local access, SMB signing enforcement, and the

planned isolation of the Smart TV, has substantially reduced the network's attack surface and established a more resilient and secure environment for all connected devices.