The Phantom Network: Isolating IoT Threats

Define the Scope

The objective of this project is to create dedicated 2.4 GHz and 5 GHz networks exclusively for Internet of Things (IoT) devices. The purpose of this segmentation is to isolate these devices—and their associated vulnerabilities, which often cannot be fully mitigated due to limited user interfaces or lack of firmware updates—from the primary home network. This segmentation strategy is intended to reduce the overall attack surface and improve network security posture.

The following IoT devices were relocated to the isolated networks and subsequently scanned using Nessus Essentials to identify potential vulnerabilities:

Vizio 65” Smart TV – 192.168.xxx.xxx

Vizio 55” Smart TV – 192.168.xxx.xxx

Ecobee 3 Smart Thermostat – 192.168.xxx.xxx

HP DeskJet 2700 Series Printer – 192.168.xxx.xxx

Feit Color-Changing Smart Light Bulbs (x9) – Assigned individual IPs beginning with 192.168.*

Set Up IoT Networks

Using the built-in IoT Network feature on my TP-Link AX3000 (Archer AX55) router, I created two dedicated wireless networks: DroidVault (2.4 GHz) and DroidVault_5G (5 GHz). These networks were configured with strong, unique passwords and secured using WPA3-Personal + WPA2-PSK [AES] encryption. This hybrid mode ensures compatibility for older IoT devices that may not support WPA3, while still allowing newer devices to benefit from stronger WPA3 encryption.

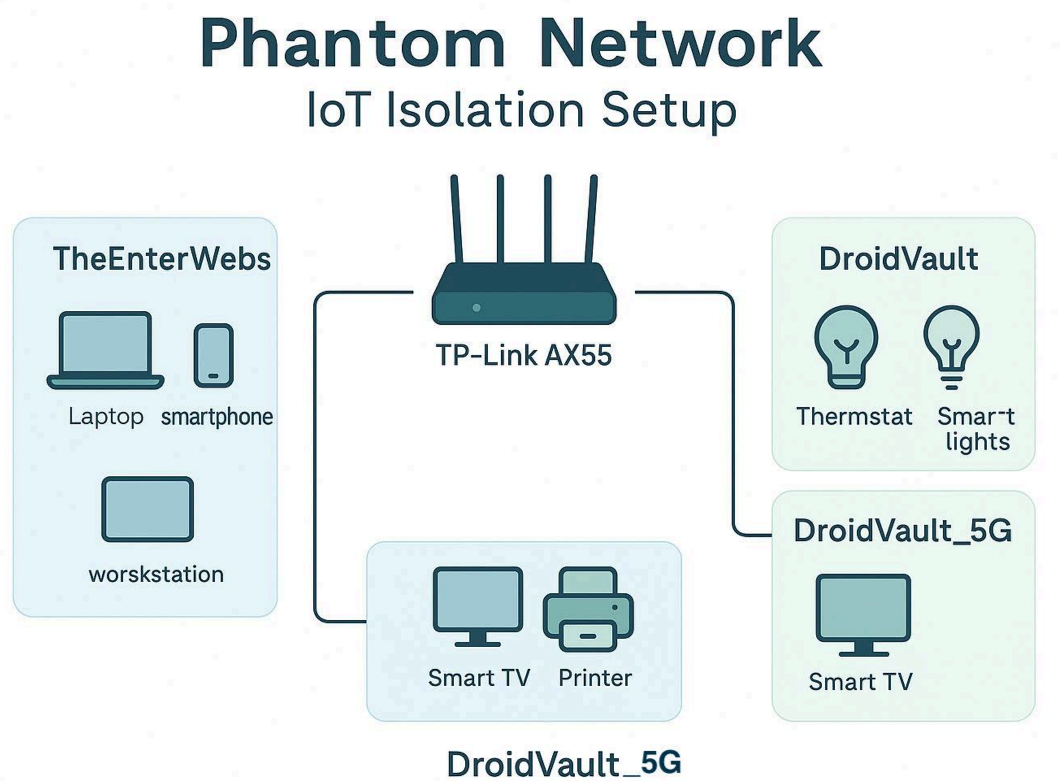
Move Devices to IoT Network

After creating the dedicated IoT networks, I connected each device based on its supported connectivity—either the 2.4 GHz (DroidVault) or 5 GHz (DroidVault_5G) band—using DHCP for automatic IP address assignment. Devices included smart TVs, a thermostat, a wireless printer, and nine smart lightbulbs.

Once all devices were successfully moved to the IoT networks, I enabled device isolation through the router's IoT Security settings. This feature restricts communication between the IoT network and the primary home network, preventing lateral movement in the event that an IoT device is compromised. Despite the isolation, all grouped IoT devices (such as the lights) continued to function together seamlessly within their own network.

To confirm that isolation was effective, I used the Linux command line interface (CLI) to attempt to ping the IoT device IPs from a system on the main network and verified that they were no longer reachable.

The diagram below illustrates the final segmented layout of the main and IoT networks following device assignment and isolation.



Scanning the Isolated Devices

With all IoT devices successfully segmented onto their respective networks, I used Nessus Essentials to perform vulnerability assessments directly from within each IoT segment. I utilized the Advanced Scan template, which offers granular control over how targets are scanned.

Two scans were configured:

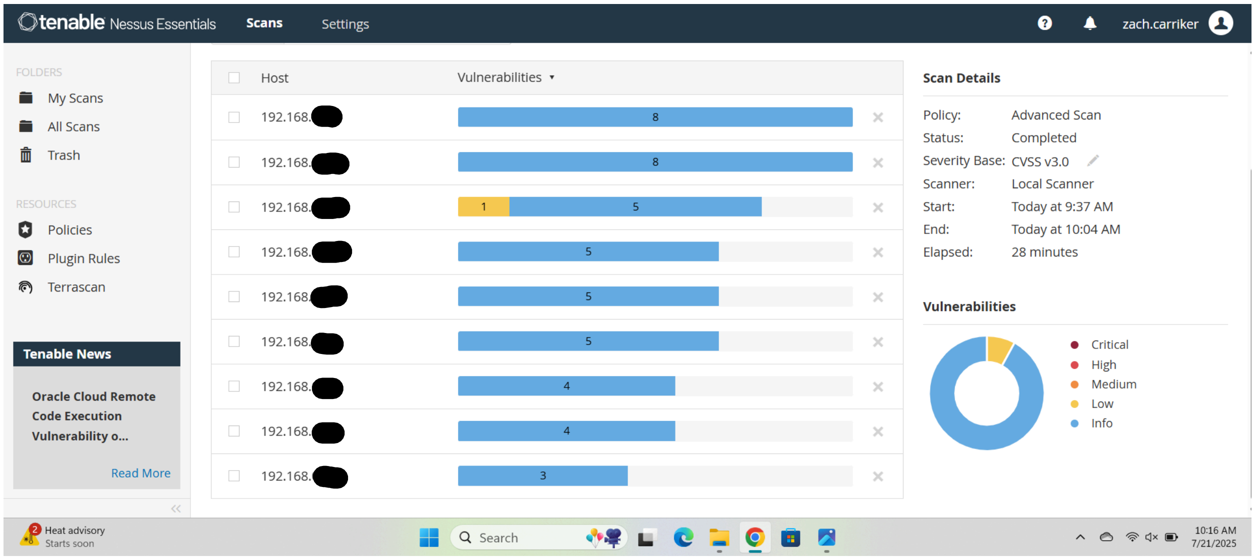
2.4 GHz IoT Scan — Included nine Feit color-changing smart lights and an Ecobee 3 Smart Thermostat.

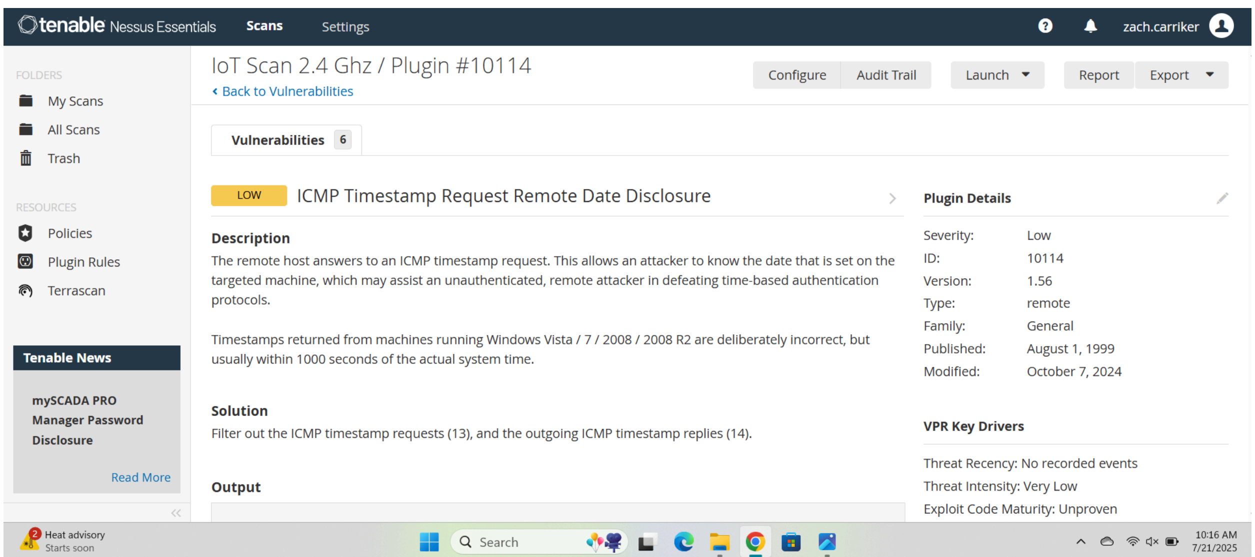
5 GHz IoT Scan — Included two Vizio Smart TVs and an HP DeskJet 2700 Series printer.

For both scans, I manually entered the IP addresses of the target devices and enabled random scan order to reduce load-related errors. Additionally, I enabled the Scan Network Printers setting in the 5 GHz scan to ensure accurate assessment of the HP printer.

To execute the scans, I connected my laptop to each IoT network as needed, confirming that all devices were reachable within their isolated segments. This ensured Nessus could perform a full evaluation, allowing me to identify and document any vulnerabilities that remain after network segmentation.

2.4 GHz IoT Network Scan Results



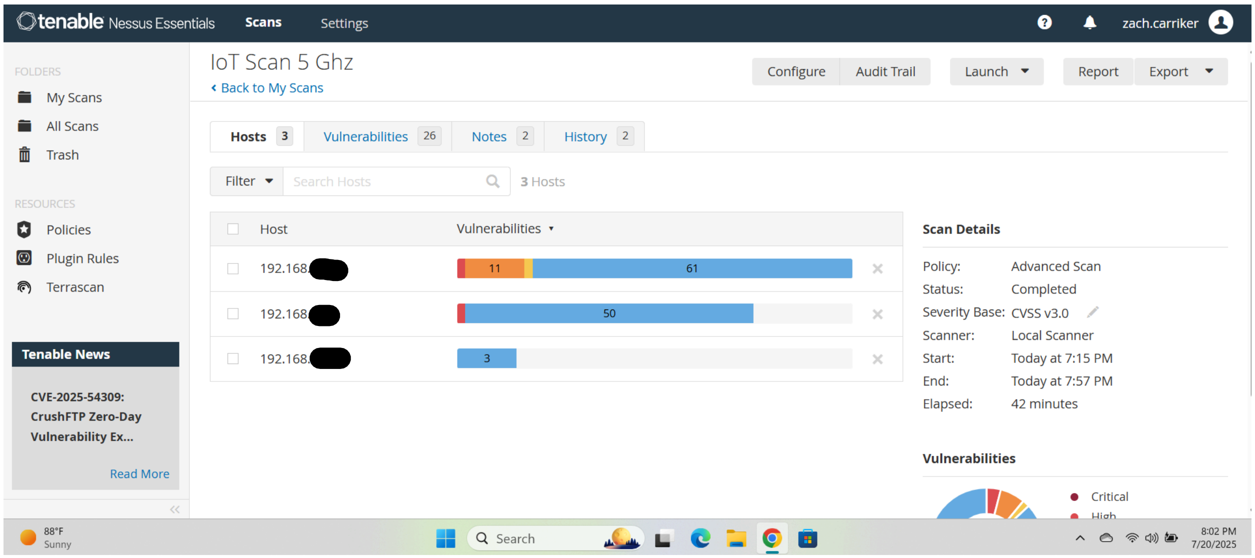


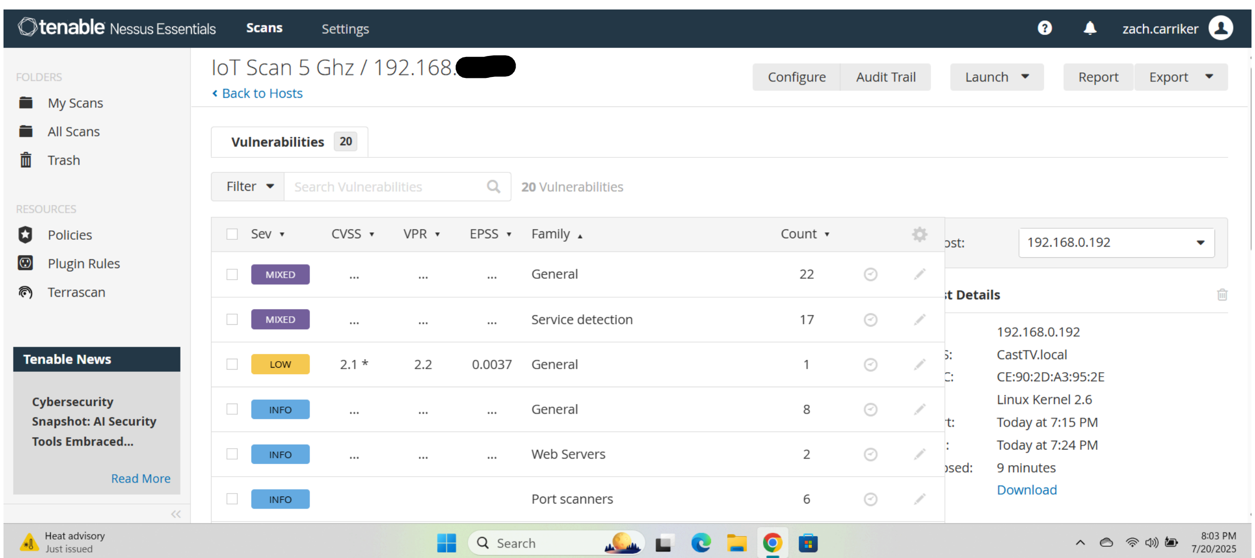
The Nessus Essentials scan of my 2.4 GHz IoT network revealed a total of six vulnerabilities, most of which were classified as low severity. The most notable finding was the “ICMP Timestamp Request Remote Data Disclosure” (Plugin #10114). This result was expected, as ICMP echo requests (ping) are permitted within the internal network for diagnostic purposes. I’ve already confirmed that these devices are not accessible via ping from outside the network, meaning this particular vulnerability would only pose a risk if an attacker were already present within the isolated IoT segment.

To mitigate the ICMP timestamp disclosure, it is recommended to block ICMP timestamp requests (type 13) and replies (type 14) within internal network segments. While this vulnerability is low risk in the current setup, addressing even minor issues contributes to a stronger overall security posture—especially in segmented environments where internal threats remain a concern.

That said, placing these devices on a separate IoT network ensures that any weaknesses identified are effectively contained. This layer of isolation prevents exposure to the main home network and limits the ability of a threat actor to move beyond the IoT environment, thereby enhancing the overall resilience of the network.

5 GHz IoT Network Scan Results





tenable Nessus Essentials Scans Settings zach.carriker

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

Tenable News

Cybersecurity Snapshot: AI Security Tools Embraced...

Read More

IoT Scan 5 Ghz / Plugin #42873

‹ Back to Vulnerability Group

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 20

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

Heat advisory Just issued | Search | 8:03 PM 7/20/2025

tenable Nessus Essentials Scans Settings zach.carriker

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

Tenable News

OCI, Oh My: Remote Code Execution on Oracle Cloud ...

Read More

IoT Scan 5 Ghz / Plugin #51192

‹ Back to Vulnerability Group

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 20

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:

Heat advisory Just issued | Search | 8:03 PM 7/20/2025

tenable Nessus Essentials Scans Settings zach.carriker

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

Tenable News

Oracle July 2025 Critical Patch Update Addresses 1...

Read More

IoT Scan 5 Ghz / Plugin #104743

‹ Back to Vulnerability Group

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 20

MEDIUM **TLS Version 1.0 Protocol Detection**

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.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

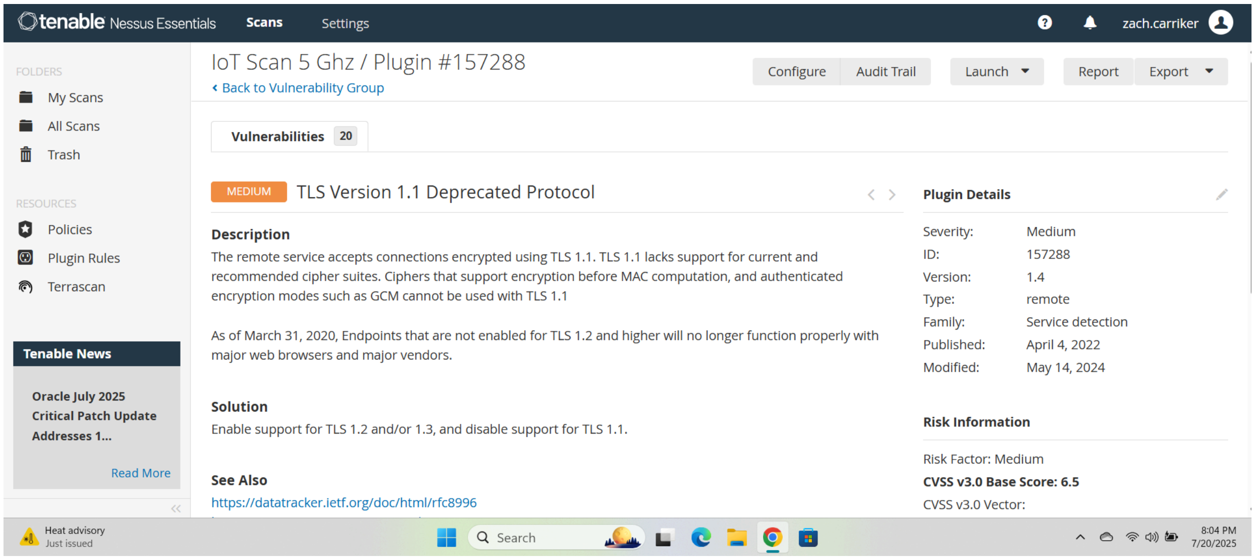
Plugin Details

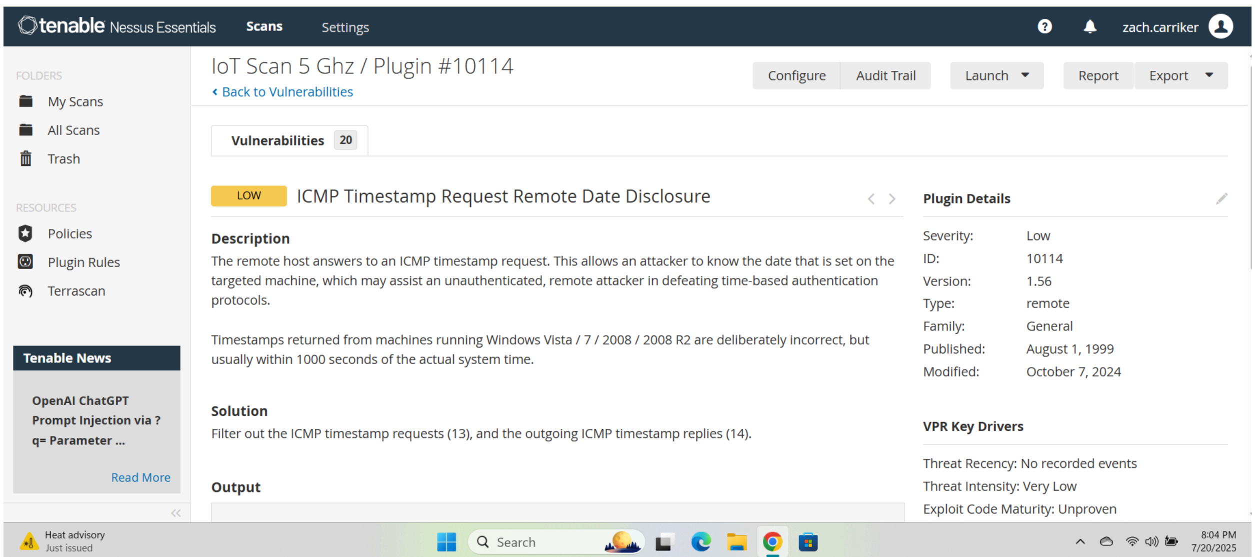
Severity: Medium
ID: 104743
Version: 1.10
Type: remote
Family: Service detection
Published: November 22, 2017
Modified: April 19, 2023

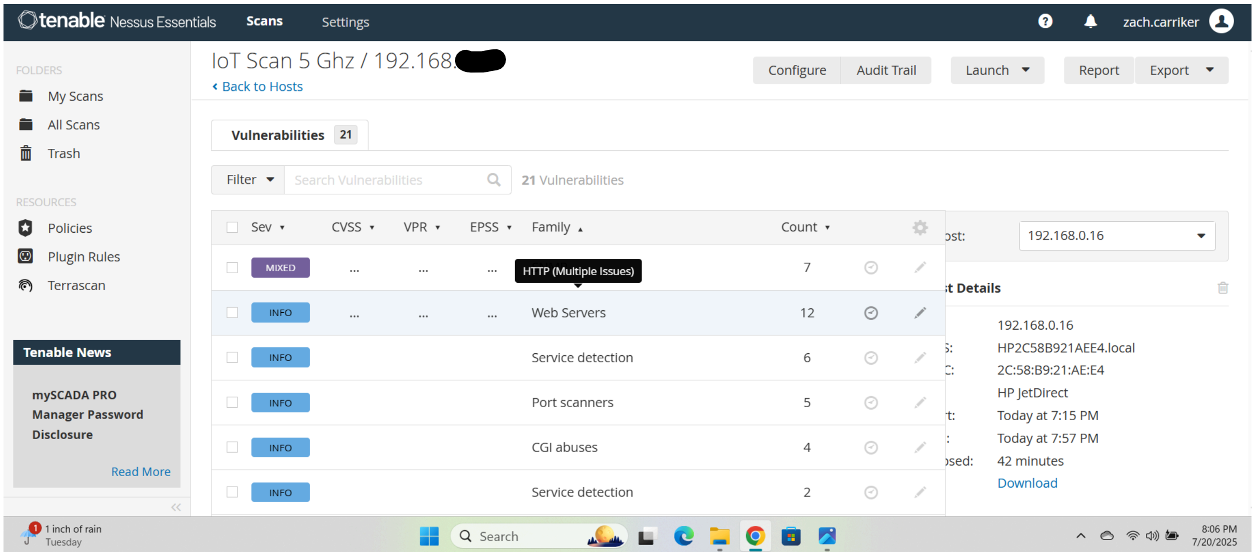
Risk Information

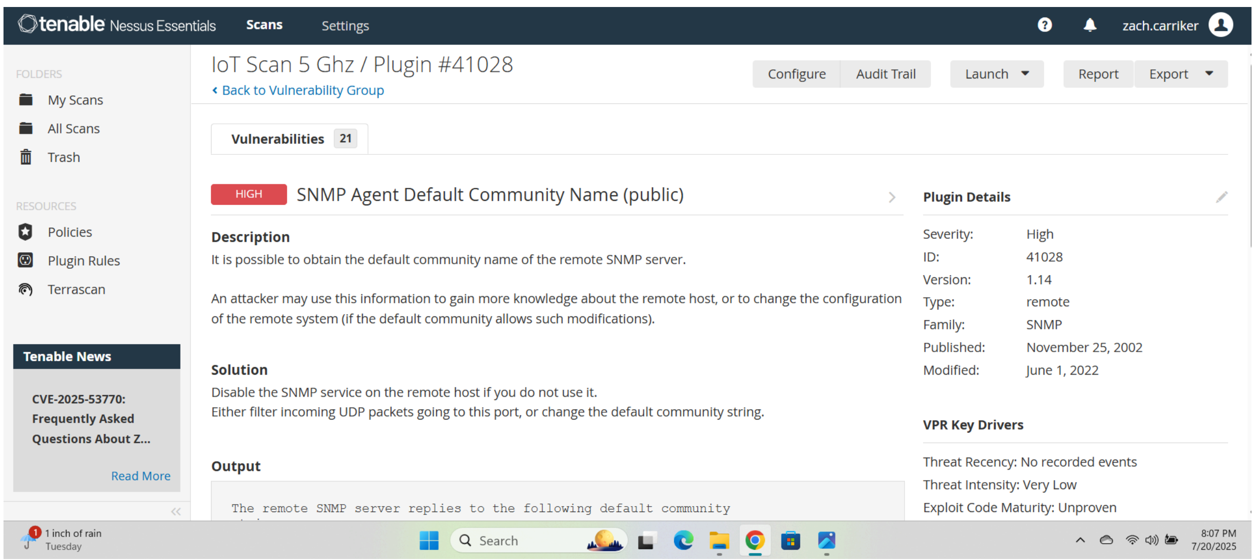
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:

Heat advisory Just issued | Search | 8:03 PM 7/20/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
IoT Scan 5 Ghz / Plugin #157288
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle July 2025 Critical Patch Update Addresses 1...
Read More
Vulnerabilities 20
MEDIUM
TLS Version 1.1 Deprecated Protocol
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
Plugin Details
Severity: Medium
ID: 157288
Version: 1.4
Type: remote
Family: Service detection
Published: April 4, 2022
Modified: May 14, 2024
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:
Heat advisory
Just issued
Search
8:04 PM
7/20/2025


tenable Nessus Essentials
Scans
Settings
zach.carriker
IoT Scan 5 Ghz / Plugin #10114
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
OpenAI ChatGPT Prompt Injection via ? q= Parameter ...
Read More
Vulnerabilities 20
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
Heat advisory
Just issued
Search
8:04 PM
7/20/2025





A separate Nessus Essentials scan of my 5 GHz IoT network revealed a larger number of vulnerabilities—26 in total—across three hosts, including several medium and high-severity issues. Notable findings include “SNMP Agent Default Community Name (public)” (Plugin #41028), “SSL Medium Strength Cipher Suites Supported (SWEET32)” (Plugin #42873), and multiple TLS/SSL-related vulnerabilities such as “TLS Version 1.1 Deprecated Protocol” (Plugin #157288), “TLS Version 1.0 Protocol Detection” (Plugin #104743), and “SSL Certificate Cannot Be Trusted” (Plugin #51192). These vulnerabilities, particularly those involving weak encryption and outdated protocols, could potentially expose sensitive data or open pathways for exploitation if the devices were accessible from the broader home network.

However, due to the nature of these IoT devices—many of which lack user interfaces or the ability to receive firmware updates—direct remediation of these issues is not feasible. For instance, default SNMP strings cannot be changed, and legacy TLS protocols or cipher suites remain in use because no configuration options are available. The “SSL Certificate Cannot Be

Trusted” finding is also expected in this environment, as it stems from a self-signed certificate issued by the TP-Link router for internal web access—a common and benign practice in home networks.

Despite these findings, the isolation of these devices on a segmented IoT network ensures they do not pose a threat to the primary home network. This segmentation prevents lateral movement, significantly reducing the risk of broader compromise even if a vulnerability within the IoT network were to be exploited.

By pushing these vulnerable endpoints into a Phantom Network, their exposure is minimized—not because the vulnerabilities are gone, but because the devices have been hidden in plain sight, beyond the reach of the main network.

Project Summary: The Phantom Network

This project focused on improving home network security by isolating Internet of Things (IoT) devices—such as smart TVs, lights, a thermostat, and a printer—onto dedicated 2.4 GHz and 5 GHz networks using a TP-Link AX3000 router. The goal was to reduce the risk these devices pose by preventing them from interacting with the main network, where more sensitive systems are connected.

After setting up the networks with strong encryption and enabling device isolation, all IoT devices were moved and tested to confirm they were unreachable from the main network. Vulnerability scans using Nessus Essentials were then performed on each network to assess security. While some vulnerabilities were found, particularly on the 5 GHz network, most were expected due to the limited configurability of consumer IoT devices.

Ultimately, this project demonstrates how network segmentation can significantly improve home security by limiting the potential impact of vulnerable or unpatchable IoT devices.