AGC

THE CONSTRUCTION ASSOCIATION

Pen Testing with an Army of One

Keefe Andrews

Pentesting with an army of 1

Does anyone here feel like an army of one?

Session Goals, You will know:

- → Difference between pen testing and vulnerability scanning
- → Why you should do pen tests
- → Know how to act on the results
- → Evaluate pen test providers

Who makes up your infosec team?

- Fully outsourced
- Just me, I wear all the hats
- Shared responsibility, no role
- Dedicated role(s)
- You need an infosec team?

Definitions

Vulnerability Scanning
vs
Penetration Testing

Vulnerability Scan

A vulnerability scan is an automated process that systematically identifies weaknesses in a system, network, or application.

It relies on specialized tools to scan for known vulnerabilities without actively attempting to exploit them.

The primary goal is to provide a comprehensive inventory of potential security issues. - CoPilot AI

PenTest

In a penetration test, experts simulate real-world attacks to

identify vulnerabilities and actively attempt to to exploit them. Pen tests go beyond mere identification; they assess the impact and risk associated with each vulnerability.

By mimicking the tactics of malicious actors, pen testers provide a more accurate picture of an organization's security posture. -CoPilot AI

Does your company conduct Pen Tests?

0
No testing at all

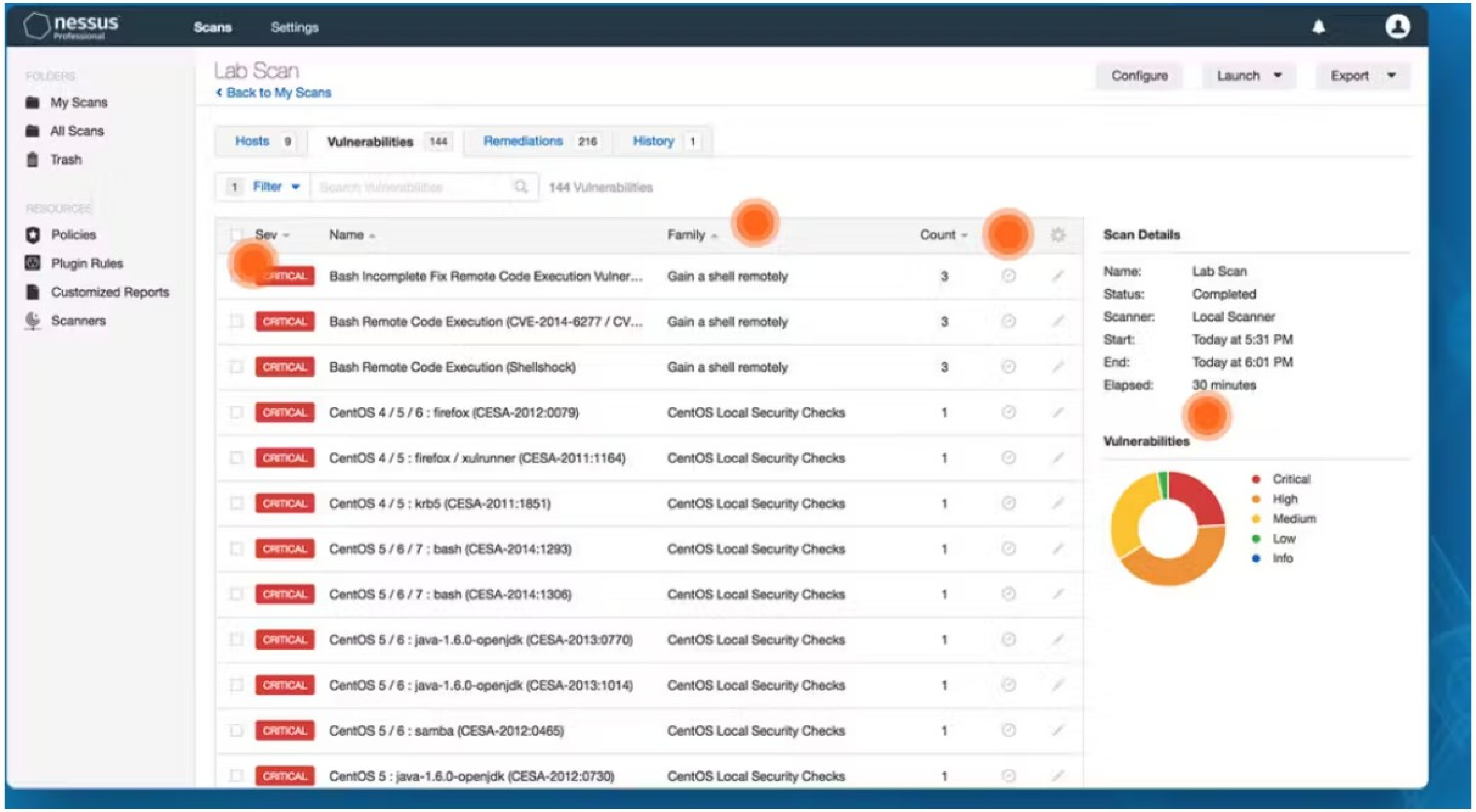
0
No. just vulnerability scans

0
Yes, every few years

0
Yes, annually

0
Multiple times a year

Why Pen Tests?



Lab Scan

‹ Back to My Scans

144 Vulnerabilities

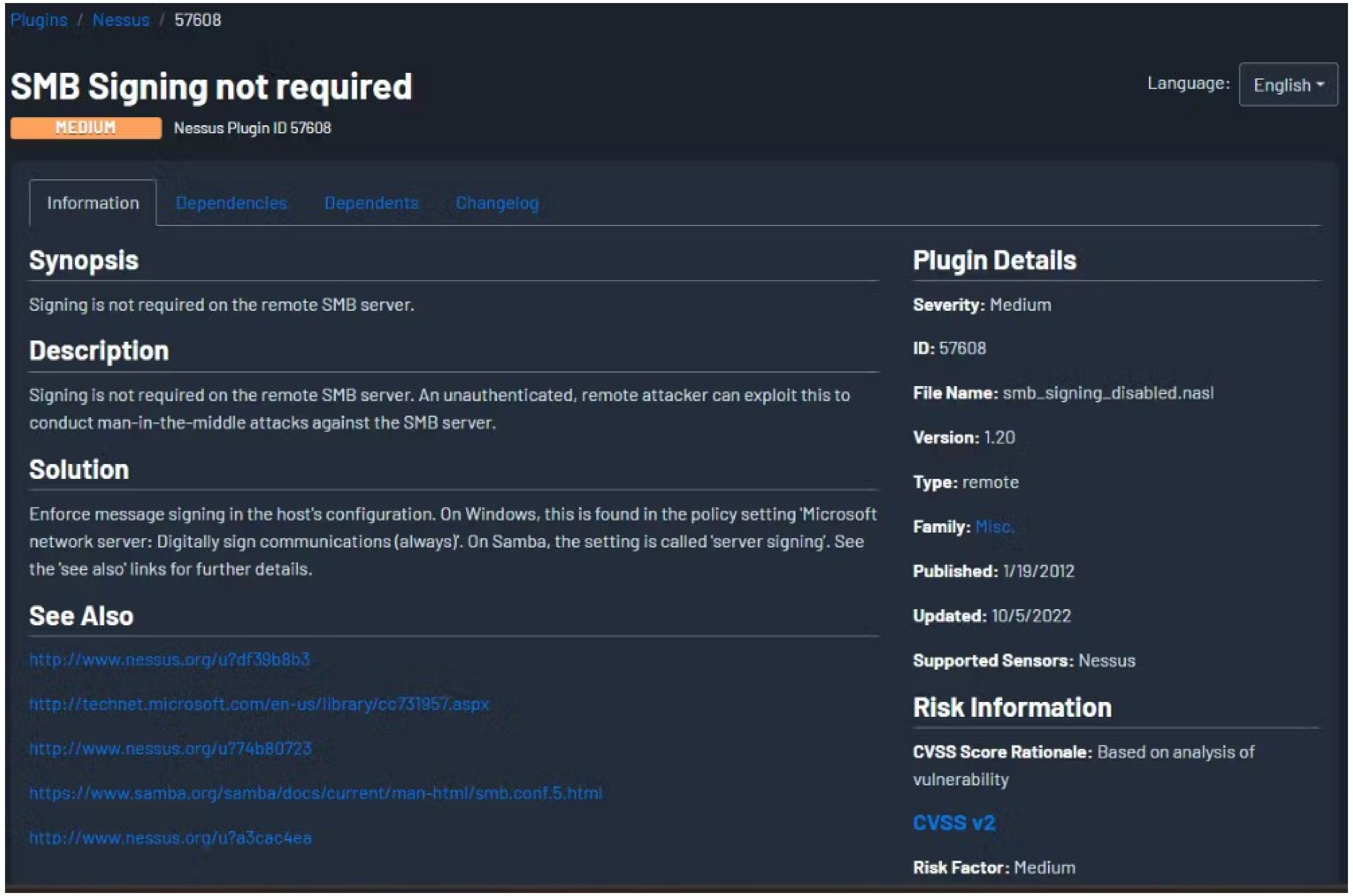
□	Sev	Name	Family	Count
□	CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
□	CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
□	CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
□	CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
□	CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1

Scan Details

Name: Lab Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 5:31 PM
End: Today at 6:01 PM
Elapsed: 30 minutes

Vulnerabilities

Is this really bad or not?



Plugins / Nessus / 57608

SMB Signing not required

MEDIUM Nessus Plugin ID 57608

Language: English

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Plugin Details

Severity: Medium

ID: 57608

File Name: smb_signing_disabled.nasl

Version: 1.20

Type: remote

Family: Misc.

Published: 1/19/2012

Updated: 10/5/2022

Supported Sensors: Nessus

Risk Information

CVSS Score Rationale: Based on analysis of vulnerability

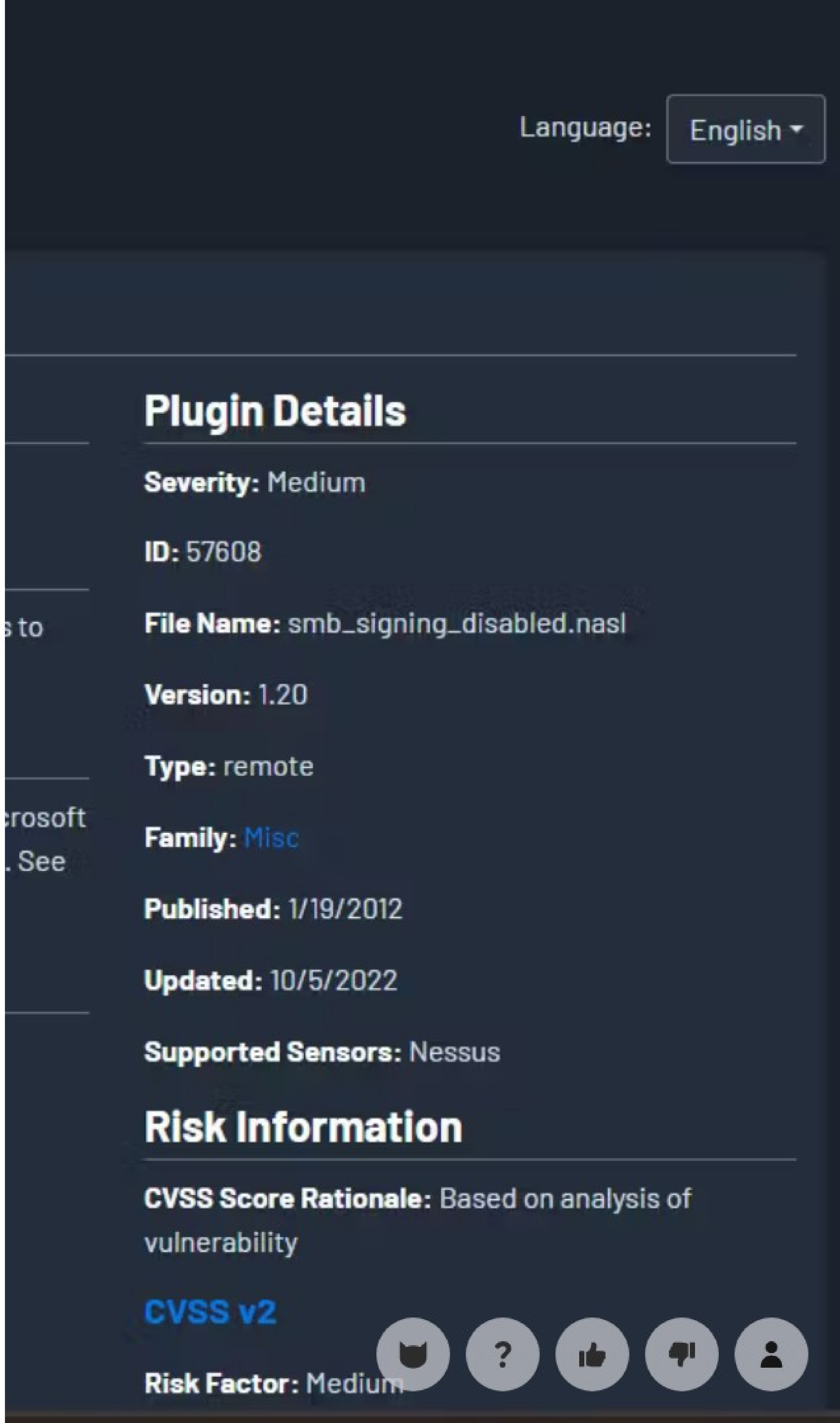
CVSS v2

Risk Factor: Medium

What about this one?

How critical is it to fix this vulnerability?

0	0	0	0	0
Not important	Probably needs to be fixed eventually	Needs to be fixed this month	Critical, fix now!	I'm not sure



Language: English

s to

rosoft
. See

Plugin Details

Severity: Medium

ID: 57608

File Name: smb_signing_disabled.nasl

Version: 1.20

Type: remote

Family: Misc

Published: 1/19/2012

Updated: 10/5/2022

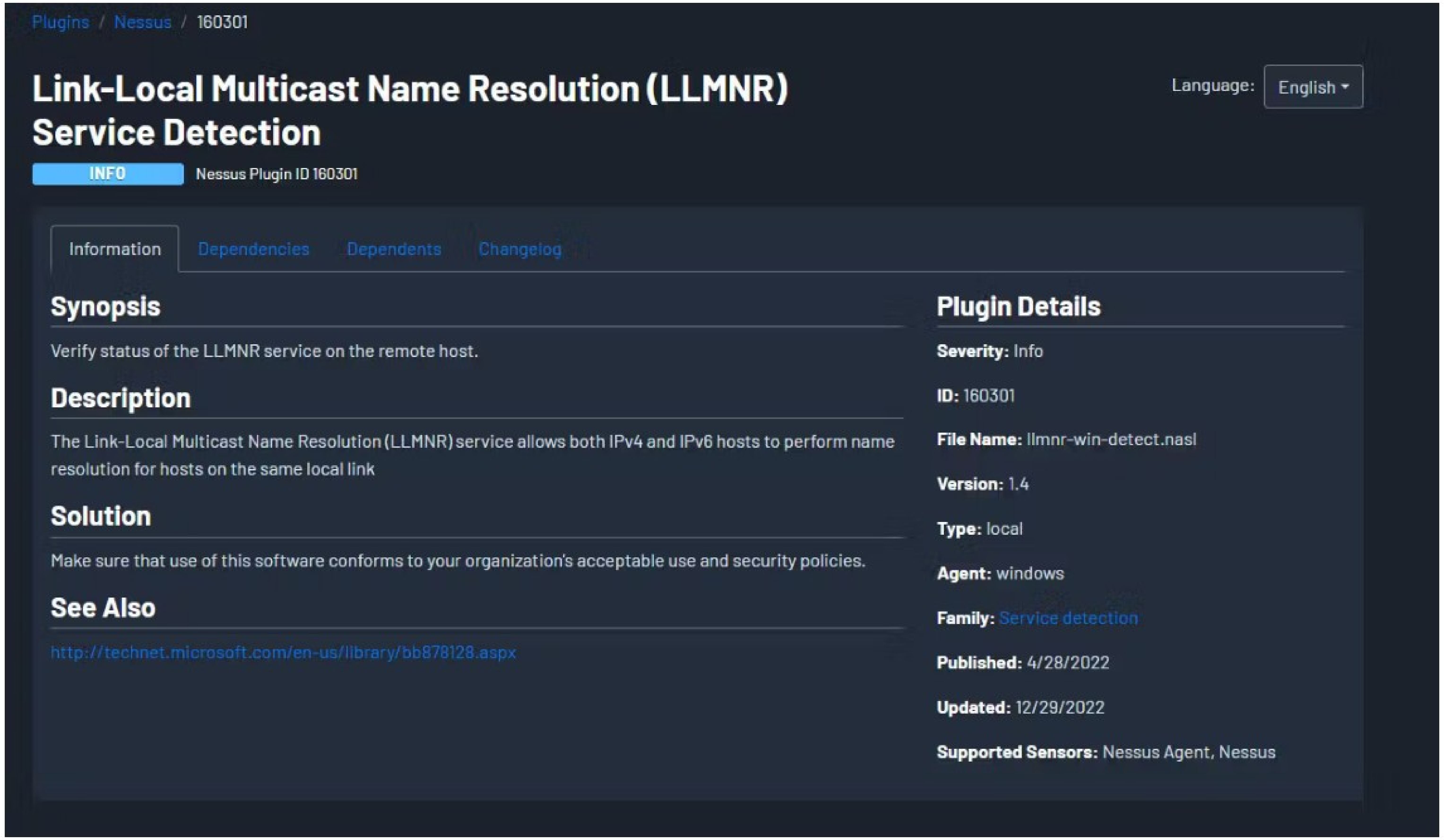
Supported Sensors: Nessus

Risk Information

CVSS Score Rationale: Based on analysis of vulnerability

CVSS v2

Risk Factor: Medium



Plugins / Nessus / 160301

Link-Local Multicast Name Resolution (LLMNR) Service Detection

INFO Nessus Plugin ID 160301

Synopsis

Verify status of the LLMNR service on the remote host.

Description

The Link-Local Multicast Name Resolution (LLMNR) service allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

See Also

http://technet.microsoft.com/en-us/library/bb878128.aspx

Plugin Details

Severity: Info

ID: 160301

File Name: llmnr-win-detect.nasl

Version: 1.4

Type: local

Agent: windows

Family: Service detection

Published: 4/28/2022

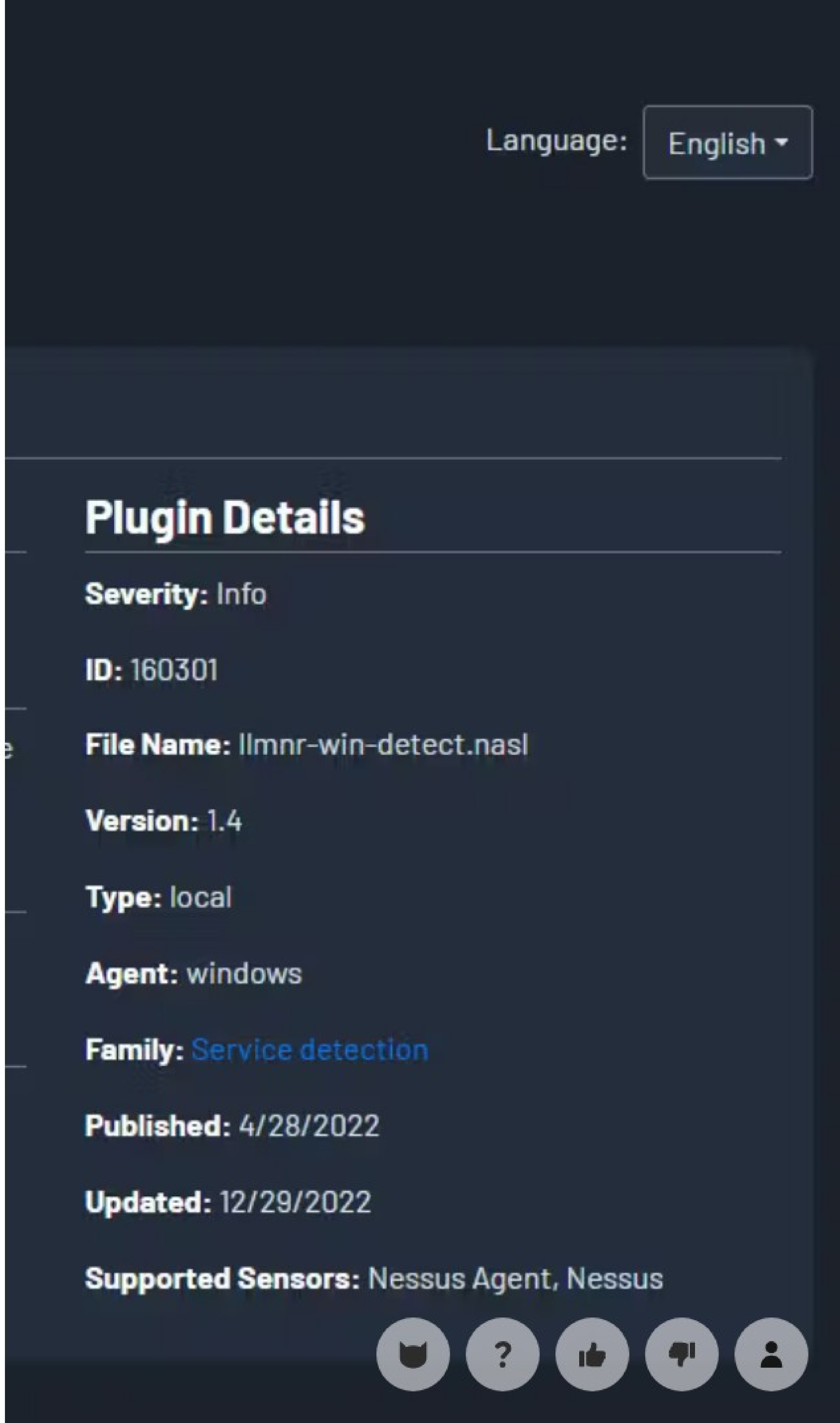
Updated: 12/29/2022

Supported Sensors: Nessus Agent, Nessus

What about this one?

How critical is it to address this, if at all?

Not important	Probably needs to be fixed eventually	Needs to be fixed this month	Critical, fix now!	I'm not sure
0	0	0	0	0



Language: English

Plugin Details

Severity: Info

ID: 160301

File Name: llmnr-win-detect.nasl

Version: 1.4

Type: local

Agent: windows

Family: Service detection

Published: 4/28/2022

Updated: 12/29/2022

Supported Sensors: Nessus Agent, Nessus

NodeZero™
Pentests
External Assets
Runners
Templates
Rapid Response
Spa

2022-02-20 | Colo and Hou D...

Impacts 26
Weaknesses 38
Credentials 14
Data 27
Hosts 68
Subdomains 3
Services 871
URLs 73
Certificates 60
Users 840
Compare

Summary

On Monday, Feb 20 2023, Anthony Castano of SpawGlass conducted an autonomous internal pentest using NodeZero. The pentest was launched from 1[redacted] at 7:30PM UTC and lasted 2 hours and 24 minutes before it completed at 9:53PM UTC.

NodeZero identified critical impacts during the pentest:

1. Host Compromise: Executed man-in-the-middle attacks that led to remote code execution and host compromise on 1[redacted].spawglass.com). Host compromise can allow attackers to gain access to sensitive information, maintain persistence within your network, and obtain lateral movement within your networks.
2. Domain User Compromise: Compromised the domain user account for C.Rushing. Once a domain user is compromised, anything that user account has access to should be considered compromised.
3. Ransomware Exposure: Compromised credentials with write access to data stores on [redacted].com) and 1[redacted]-[redacted].com). These assets are vulnerable to a ransomware attack. Ransomware is used by attackers to encrypt business-critical data with a secret key, then demand a ransom payment from your company before releasing the key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and all affected services restored.

Fixing the following weaknesses will reduce the organization's cyber risk.

View More

Overall Exposure Level

NodeZero found 26 attack paths
Compromise, Domain User Comp
Exposure and Sensitive Data Expo

26 Impacts

38 Weaknesses

14 Credentials

1 Compromised Host

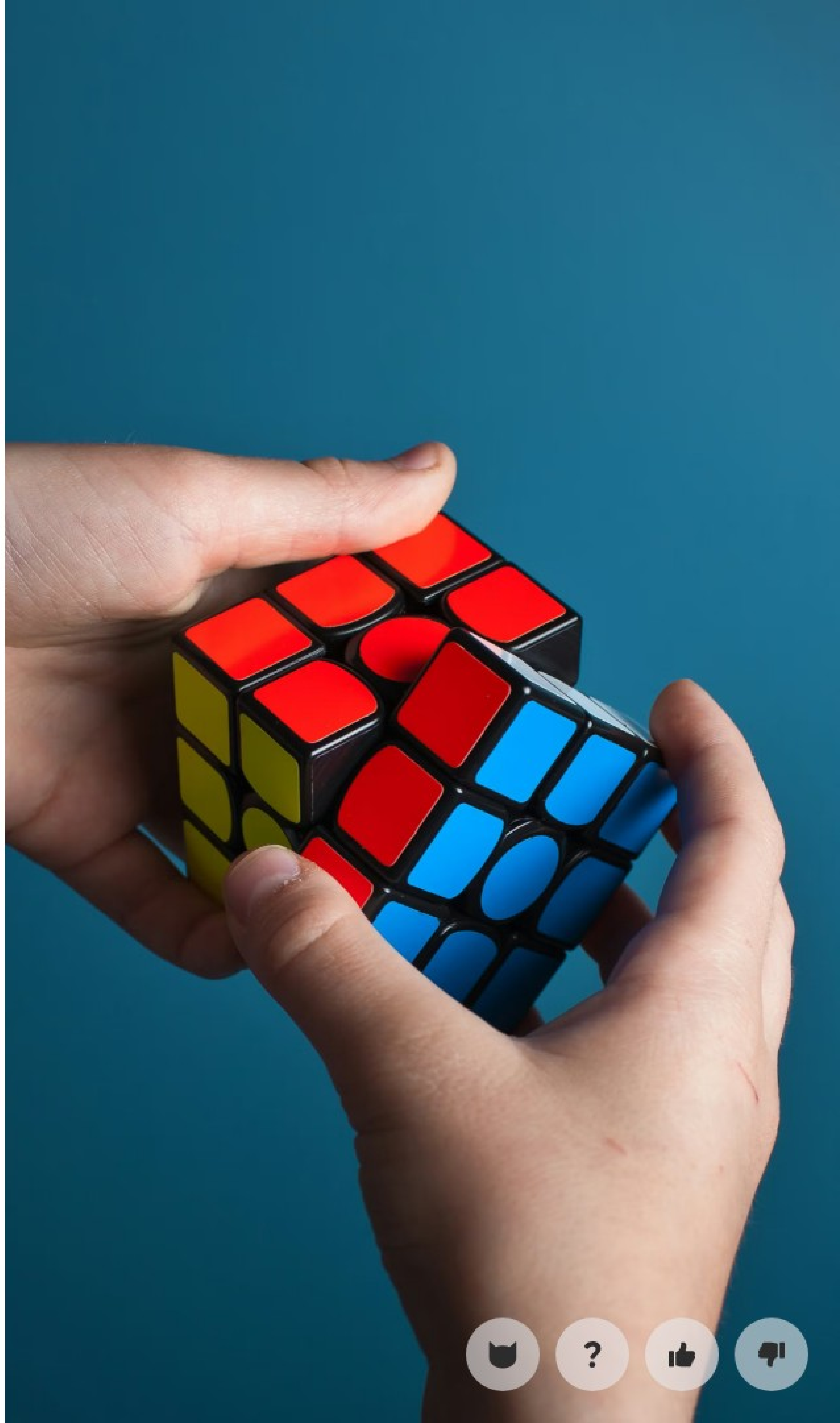
MITRE ATT&CK®

Top Weaknesses and Impacts

Select an impact or weakness to read about the relationship between Impacts and Weaknesses.

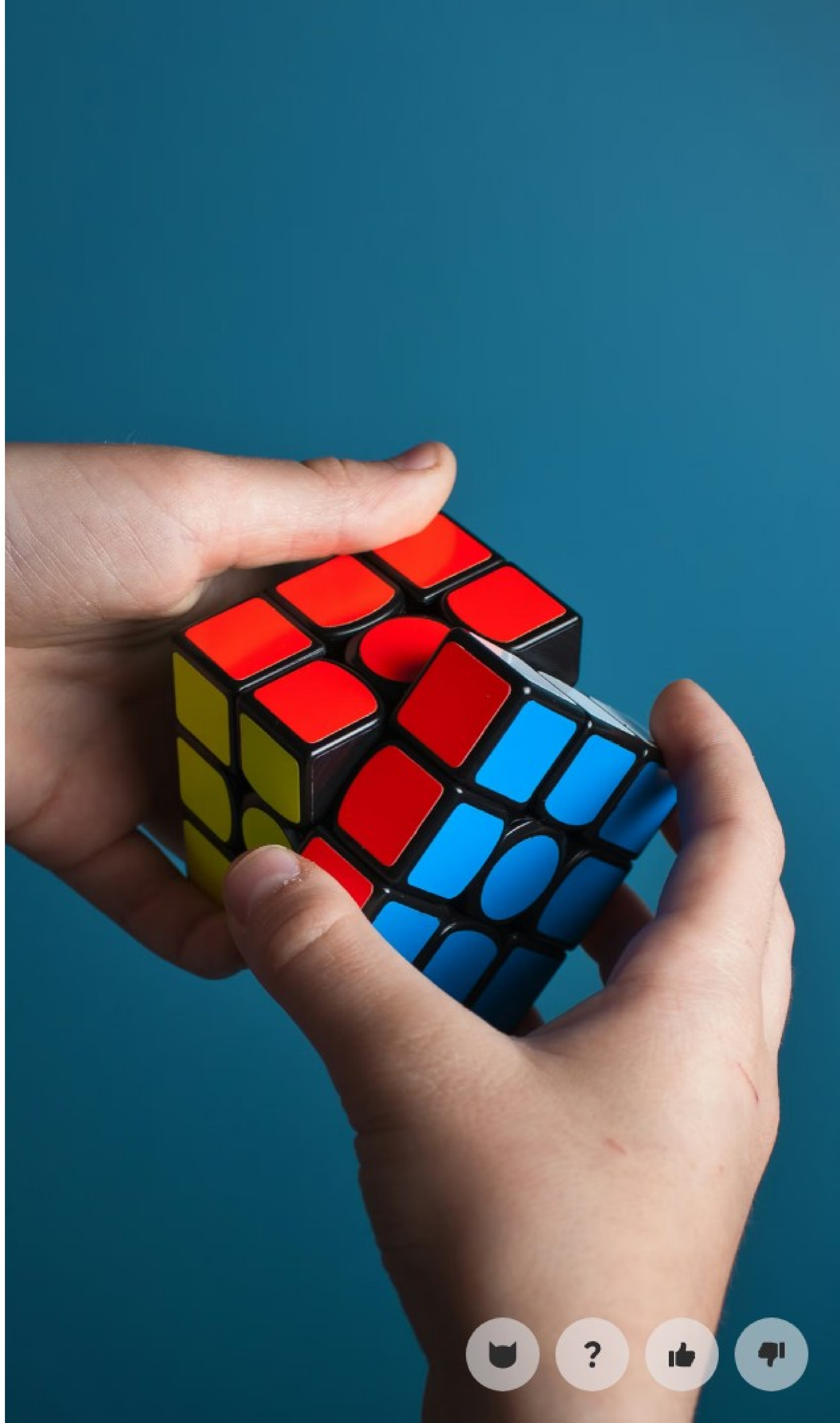
This chart displays the amount of weakness to amount of impact type relationship that exists within your Impact Categories.

How easy is it to fix LLMNR?



Nessus Information Link LLMNR

https://learn.microsoft.com/en-us/previous-versions//bb878128(v=technet.10)?redirectedfrom=MSDN



How do I fix SMB signing or turning off LLMNR?

SpawGlass' Journey

- Vulnerability Patching Only
- Light Pen Testing
- Full Server Network Pen Testing
- Maintenance and Deviation Detection

Selection of a partner

- Automated Testing
- Actionable Information
- Affordable Pricing

using a custom cron expression. Learn More

Schedule Name *

Pentest Template *
Select...

Run Every Week at 12:00 AM

Repeat On S M T W T F S

Advanced Options: CRON Expression ○

At 12:00 AM, every day.
Next: Jul 29, 2024, 12:00 AM UTC (Local: Jul 28, 2024, 7:00 PM CDT)

ng to critical impacts, including a **Host Compromise** [redacted].com).

7 BASE SCORE

5 ATTACK PATHS

ate **19%** of critical impact paths.

e of two components of Microsoft Windows machines that serve as can spoof a reply as an authoritative source to a victim request and etwork. Credential information can be captured in hashed or plaintext

discover the plaintext password for reuse on other systems or the ns as well. Likewise, a captured plaintext credential can be

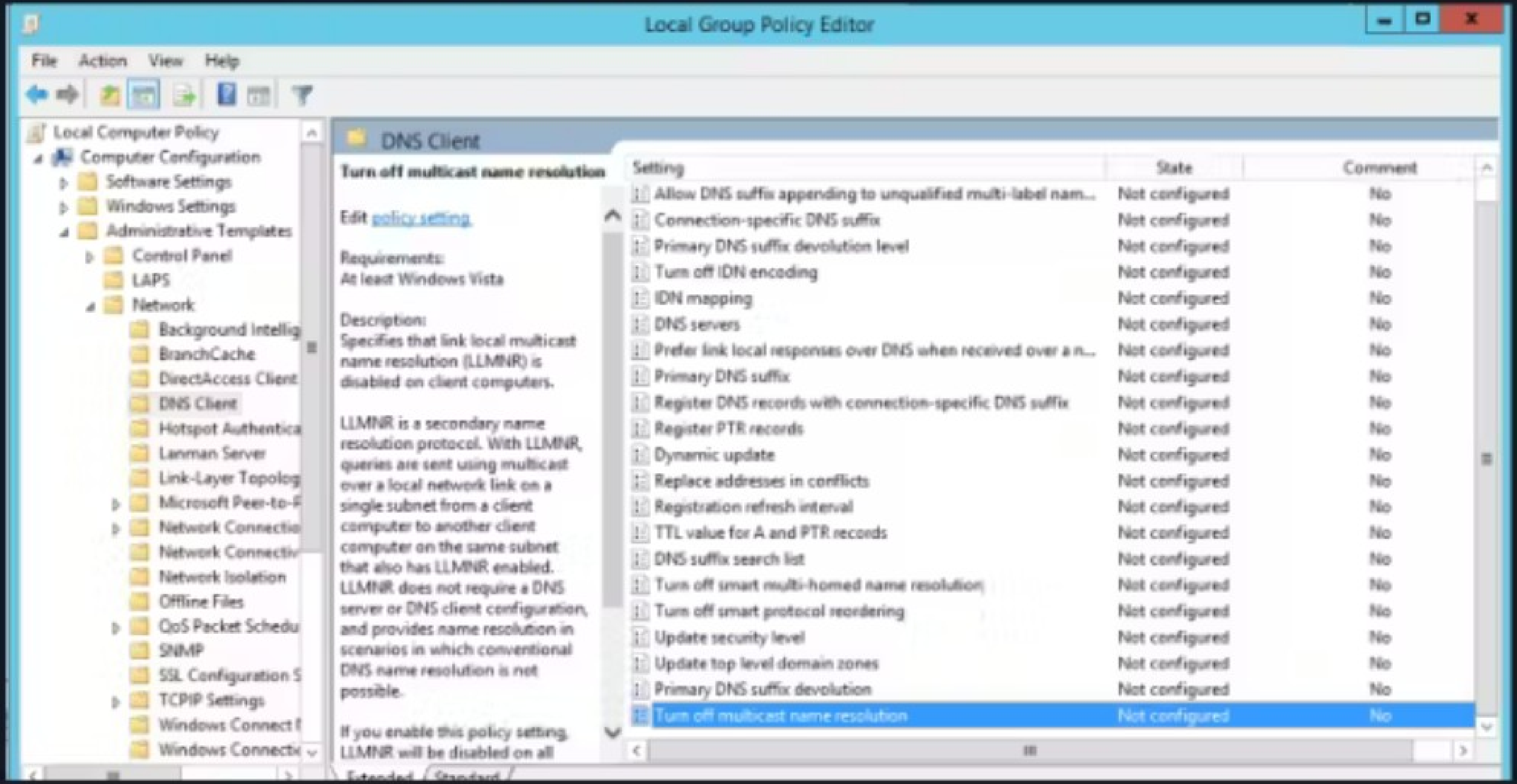
S Poisoning

Proofs 7 | **Fix Actions** | Downstream Impacts 5 | Credentials 14

Table of Contents

Option 1: Disable via Group Policy.

1. Open the “Local Group Policy Editor” on the Domain Controller.
2. Navigate to Computer Configuration > Administrative Templates > Network > DNS Client and then selecting “Turn Off Multicast Name Resolution”



Turn off multicast name resolution

Edit policy setting.

Requirements:
At least Windows Vista

Description:
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, LLMNR will be disabled on all

Setting	State	Comment
Allow DNS suffix appending to unqualified multi-label nam...	Not configured	No
Connection-specific DNS suffix	Not configured	No
Primary DNS suffix devolution level	Not configured	No
Turn off IDN encoding	Not configured	No
IDN mapping	Not configured	No
DNS servers	Not configured	No
Prefer link local responses over DNS when received over a n...	Not configured	No
Primary DNS suffix	Not configured	No
Register DNS records with connection-specific DNS suffix	Not configured	No
Register PTR records	Not configured	No
Dynamic update	Not configured	No
Replace addresses in conflicts	Not configured	No
Registration refresh interval	Not configured	No
TTL value for A and PTR records	Not configured	No
DNS suffix search list	Not configured	No
Turn off smart multi-homed name resolution	Not configured	No
Turn off smart protocol reordering	Not configured	No
Update security level	Not configured	No
Update top level domain zones	Not configured	No
Primary DNS suffix devolution	Not configured	No
Turn off multicast name resolution	Not configured	No

?

Watch out for…

- Branded Nessus scans
- Vague details of tools used
- No after scan support

Continue your learning, recommended podcasts:

- → Heavy Strategy
- → Security Now
- → Packet Protector
- → Visit with Horizon3.ai

Questions?