Vulnerability Assessment Report

Cat Company

Prepared by: Prinson D'silva
Date: January 23rd, 2025

Table of Contents

Executive Summary

The vulnerability assessment scan was conducted for Cat company on January 23, 2025 in an attempt to identify and mitigate security weaknesses within their IT infrastructure.
The scan was conducted using the full and fast configuration of OpenVAS across two environments (LinuxServer and Windows11) to find potential weaknesses such as coding flaws, unprotected open ports, misconfigurations, missing patches and weak passwords, etc. A total of 20 vulnerabilities were revealed which were categorized based on their severity, with a focus on addressing those with a standards based Common Vulnerability Scoring System (CVSS) score greater than 1.0.

Key findings included two main vulnerabilities:

- Medium Severity (CVSS: 5.0): A vulnerability related to DCE/RPC and MSRPC service enumeration was detected on the Windows11 machine (port 135/tcp), which could allow attackers to gather information about the host.
- Low Severity (CVSS: 2.6): TCP timestamp information disclosure was found on both the LinuxServer and Windows11 machines, potentially revealing system uptime and other details that could aid attackers.

Based on the Risk Assessment, the following actions for mitigation are recommended in priority order:

I. Short-term Mitigations:
    - For Medium Severity: Implement network segmentation to isolate critical systems and block port 135 (RPC) on the firewall to limit exposure.
    - For Low Severity: Disable TCP timestamps and, if possible, randomize timestamp offsets to reduce information leakage.

II. Long-term Mitigations:
    - Access Control: Ensure that only authorized systems can access sensitive services.
    - Patch Management: Regularly update systems to mitigate vulnerabilities.
    - Monitoring: Implement systems to detect unusual network activity, especially related to port 135.
    - Security Awareness: Educate users and administrators about potential risks and mitigation strategies.

By addressing these vulnerabilities, we can significantly enhance our security posture and reduce the risk of exploitation, ensuring continued safe business operations in alignment with industry standard frameworks and guidelines.

Scan Results

The purpose of this project was to find security vulnerabilities in our systems. According to IBM, a security vulnerability is any weakness in the structure, function or implementation of an IT asset or network which can be exploited by hackers or threat actors to gain unauthorized access and cause harm to the network, users or the business. [Kosinski M., December 2023]

This report was put together based on the output of the Vulnerability Assessment scan which was conducted on January 23rd, 2025.

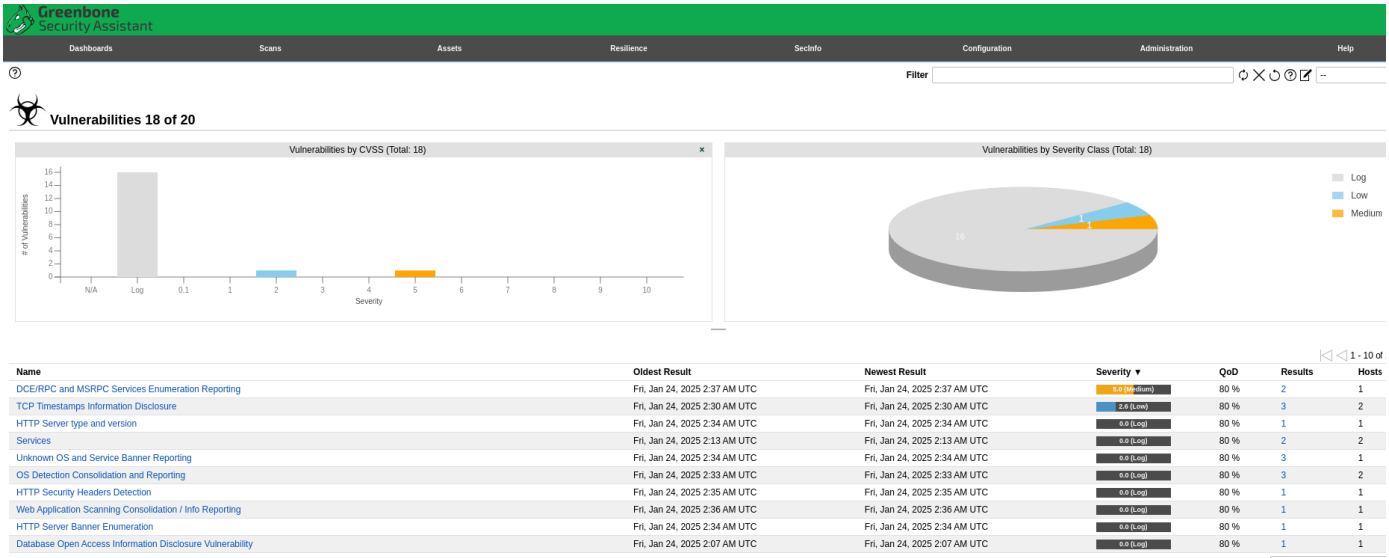

Fig. 1: Scan results from OpenVAS

The vulnerabilities found in the results of this scan were classified into several categories referred to as “Severity Classes” by the Common Vulnerability Scoring System (CVSS) which is a method used to supply a qualitative measure of severity which are denoted by a number from 0.0 to 10.0 [NIST, September 2024].

A higher score indicates a more severe vulnerability that demands immediate attention, and a lower score suggests a less critical issue. As mentioned by Crowdstrike, we have categorized vulnerability scores as follows:

- Low severity (1.0 to 3.9): Poses minimal risk and often requires specific conditions to be exploited.
  Medium severity (4.0 to 6.9): More common and might be easier to exploit but typically don't lead to severe consequences.
- High severity (7.0 to 8.9): A significant threat, often allowing unauthorized access or control over affected systems.
- Critical severity (9.0 to 10): The most dangerous vulnerabilities, usually allowing widespread exploitation with severe impacts like data loss, system downtime, or complete system takeover.

Our scans detected around twenty vulnerabilities in total (as seen in Fig. 1) out of which two had a score greater than 1.0 and needed to be addressed - which would be discussed further in the report.

Methodology

Tools

For conducting Vulnerability scans in our project, we used **OpenVAS** (Open Vulnerability Assessment Scanner) developed by Greenbone Technologies, which is a full-featured scan engine that executes Vulnerability Tests (VTs) against target systems.

This tool was used to find potential weaknesses such as coding flaws, unprotected open ports, misconfigurations, missing patches and weak passwords, etc.

Tests

The option used to conduct the scan was **Full and fast**.

This scan configuration is based on the information gathered in the previous port scan and uses almost all VTs. Only VTs that will not damage the target system are used. VTs are optimized in the best possible way to keep the potential false negative rate especially low.

There are other "Full" configurations that only provide more value in rare cases but with much higher effort.

[GOS 22.04.26, January 2025]

Environments

The tests were run on the following environments as requested by the Cat Company:

- LinuxServer Machine: IP address - 10.0.2.15
- Windows11 Machine: IP address - 10.0.2.4

Findings

After conducting full and fast scans on the host machines, OpenVAS picked a total of 20 vulnerabilities (see Fig. 1). However due to limited resources, we are only looking to address vulnerabilities which have a score greater than 1.0 and belong to one of the Severity classes.
Hence based on the results obtained from the scan, there were two types of vulnerabilities detected which need to be addressed:

- Low Severity - 1
    - Both LinuxServer and Windows11 machines.
- Medium Severity - 1
    - Windows11 machine

The full report results are attached in Appendix 1 and Appendix 2.

Medium Severity

- DCE/RPC and MSRPC Services Enumeration Reporting - Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
  This vulnerability was detected only on the Windows11 machine.
  - Affecting Service (Port) - 135/tcp
  - Impact - Because of this vulnerability, an attacker may use this fact to gain more knowledge about the remote host.

Low Severity

- TCP Timestamps Information Disclosure: The remote host implements TCP timestamps and therefore allows to compute the uptime.
  This vulnerability was detected on both LinuxServer and Windows11 machines.
  - Affecting Service (Port) - general/tcp
  - Impact - A side effect caused by this feature is that the uptime of the remote host can sometimes be computed.

Risk Assessment

Although we have identified limited vulnerabilities to be addressed, they can certainly have an impact on some applications used in our day-to-day business operations.

Medium severity:

CVSS Score range: 4.0 to 6.9

This vulnerability is more common and might be easier to exploit but typically does not lead to severe consequences.

For example, a score of 5.5 might be given to a cross-site scripting issue that could be exploited more easily but doesn't compromise an entire system.

Low severity:

CVSS Score range: 1.0 to 3.9

This vulnerability poses minimal risk and often requires specific conditions to be exploited.

An example of a vulnerability that scores 2.0 might be a low-impact information disclosure flaw that requires high-level privileges to exploit.

[Wang B., June 2024]

Table 1: Detailed Risk Assessment

Vulnerability	Affected Target, Service, Software	CVSS Score (Severity)	Security Implications	Solution	Count
DCE/RPC and MSRPC Services Enumeration Reporting	Windows11 / 135/tcp	5.0 (Medium)	Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries by which an attacker may use this fact to gain more knowledge about the remote host.	Filter incoming traffic to this port. [Greenbone, 2018]	1
TCP Timestamps Information Disclosure	LinuxServer/ Windows11, TCP implementations that implement RFC1323/RFC7323, general/tcp	2.6 (Low)	Timestamps provide the attacker with a means to guess the operating system of the target (indicating a system that might be vulnerable due to lack of patching) or plan attack windows.	Disable TCP Timestamps. [IBM, 2023] Randomize timestamp offset. [CWE-200, 2024]	2

Recommendations

The following are the recommended mitigations based on the Risk Assessment of this findings of the vulnerability scan:

Short-term Mitigations

For Medium Severity Vulnerabilities:

- Implement Network Segmentation and Isolation - Use network segmentation to isolate critical systems and services running MSRPC/DCE/RPC from less secure parts of your network. By creating VLANs and using firewalls, you can limit the exposure of sensitive services to only authorized users or systems. [NIST, 2020]
- Block RPC Ports - If MSRPC or DCE/RPC services are not required, block port TCP 135 used by RPC on the host firewall.
    - Use Windows Command:
      New-NetFirewallRule -DisplayName "Block RPC" -Direction Inbound -Protocol TCP -LocalPort 135 -Action Block
      [Microsoft, 2025]

For Low Severity Vulnerabilities:

- Disable TCP Timestamps - Many operating systems allow disabling the TCP timestamp option, preventing the disclosure of this information. [IBM, 2023]
    - Command for LinuxServer:
      Add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime
    - Command for Windows11:
      Execute 'netsh int tcp set global timestamps=disabled'
- Randomize timestamp offset- Some systems can be configured to use a random offset when generating timestamps, making it harder for attackers to accurately calculate uptime. [CWE-200, 2024]

Long-term Mitigations

The following security policies and configurations can be implemented to mitigate these vulnerabilities in long-term: -

- Enforce Access Control:
    - Ensure that only authorized and trusted internal systems can communicate with RPC services, and limit the exposure to the internet or untrusted networks.
    - Employ the principle of least privilege across all systems to limit potential damage.
      [NIST, 2020]
- Patch Management:
    - Ensure that all systems are regularly patched to mitigate known vulnerabilities focusing on both Windows and Linux keep the operating systems and services up to date.
- Monitoring and Alerts:
    - Implement a monitoring system that detects unusual network activity, such as attempts to enumerate services over port 135. This will help

identify potential attack attempts before they result in a security breach.

- Security Awareness Training:
    - Ensure that users and administrators are aware of the risks associated with information disclosure and how to mitigate potential threats, especially concerning system uptime or unnecessary open ports.

By implementing these short-term and long-term mitigations, we can significantly reduce the risk posed by these vulnerabilities while maintaining business operations.

References

- NIST (September, 2024) - *National Vulnerability Database: Vulnerability Metrics*. NIST. Retrieved from https://nvd.nist.gov/vuln-metrics/cvss
- Bei Wang (June, 2024) - *Common Vulnerability Scoring System (CVSS).* Crowdstrike. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/common-vulnerability-scoring-system-cvss/#:~:text=Understanding%20the%20scoring%20scale%20in,have%20a%20score%20of%209.5.
- Matt Kosinski (December 2023) - *What is vulnerability scanning?.* IBM. Retrieved from https://www.ibm.com/think/topics/vulnerability-scanning
- Greenbone Enterprise Appliance Manual - GOS 22.04.26 (January, 2025) - *10.9.1 Default Scan Configurations.* Retrieved from https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html#default-scan-configurations
- Greenbone (October 2018) - *How to fix vulnerabilities which are found in OpenVAS results*. Retrieved from https://forum.greenbone.net/t/how-to-fix-vulnerabilites-which-are-found-in-openvas-results/396
- IBM (2023) - *IBM Unified Management Server for z/OS.* Retrieved from https://www.ibm.com/docs/en/umsfz/1.2.0?topic=tasks-disabling-tcp-timestamps
- CWE-200 (November 2024) - *Exposure of Sensitive Information to an Unauthorized Actor*. MITRE. Retrieved from https://cwe.mitre.org/data/definitions/200.html
- NIST Special Publication 800-53 Revision 5 (September 2020) - Security and Privacy Controls forInformation Systems and Organizations .*3.18 SYSTEM AND COMMUNICATIONS PROTECTION.* Pg. 292. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- Microsoft (January 2025) - Windows > Powershell > *NetSecurity.* Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/powershell/module/netsecurity/?view=windowsserver2025-ps

Appendices

Appendix 1: Scan Report for LinuxServer

I Summary
==========

This document reports on the results of an automatic security scan.
The report first summarises the results found.
Then, for each host, the report describes every issue found.
Please consider the advice given in each description, in order to rectify
the issue.

All dates are displayed using the timezone "Coordinated Universal Time",
which is abbreviated "UTC".

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses
the actual threat of the result.

Notes are included in the report.Information on overrides is included in the report.

This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the
filtering described above. Before filtering there were 18 results.

Scan started: Fri Jan 24 02:11:50 2025 UTC
Scan ended: Fri Jan 24 03:02:39 2025 UTC
Task: Windows11

Host Summary
****

Host	High	Medium	Low	Log	False Positive
10.0.2.4	0	1	1	0	0
Total: 1	0	1	1	0	0

II Results per Host
==========

Host 10.0.2.4
****

Scanning of this host started at: Fri Jan 24 02:12:12 2025 UTC
Number of results: 2

Port Summary for Host 10.0.2.4

Service (Port)	Threat Level
135/tcp	Medium (CVSS: 5.0)
general/tcp	Low (CVSS: 2.6)

Security Issues for Host 10.0.2.4

Issue

NVT: DCE/RPC and MSRPC Services Enumeration Reporting
OID: 1.3.6.1.4.1.25623.1.0.10736
Threat: Medium (CVSS: 5.0)
Port: 135/tcp

Summary:
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC se!
rvices running
on the remote host can be enumerated by connecting on port 135 and doing the a!
ppropriate queries.

Vulnerability Detection Result:
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p!
rotocol:
Port: 49664/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: Ngc Pop Key Service
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: Ngc Pop Key Service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2

Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: KeyIso
Port: 49665/tcp
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49665]
Port: 49666/tcp
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49666]
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49666]
Port: 49667/tcp
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49667]
Annotation: Windows Event Log
Port: 49668/tcp
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
Port: 49676/tcp
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:10.0.2.4[49676]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re!
porting this list is not enabled by default due to the possible large size of th!
is list. See the script preferences to enable this reporting.

Impact:
An attacker may use this fact to gain more knowledge
about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method:
Details:
DCE/RPC and MSRPC Services Enumeration Reporting

(OID: 1.3.6.1.4.1.25623.1.0.10736)
Version used: 2022-06-03T10:17:07Z

Issue

NVT: TCP Timestamps Information Disclosure
OID: 1.3.6.1.4.1.25623.1.0.80091
Threat: Low (CVSS: 2.6)
Port: general/tcp

Summary:
The remote host implements TCP timestamps and therefore allows
to compute the uptime.

Vulnerability Detection Result:
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4867830
Packet 2: 4869888

Impact:
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line
'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to appl!
y the settings at
runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timesta!
mps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be complete!
ly disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Tim!
estamp options when
initiating TCP connections, but use them if the TCP peer that is initiating co!
mmunication includes
them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS:
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight:

The remote host implements TCP timestamps, as defined by
RFC1323/RFC7323.

Vulnerability Detection Method:
Special IP packets are forged and sent with a little delay in
between to the target IP. The responses are searched for a timestamps. If foun!
d, the timestamps
are reported.
Details:
TCP Timestamps Information Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.80091)
Version used: 2023-12-15T16:10:08Z

References:
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url:
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.as
px?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

Appendix 2: Scan Report for Windows11

I Summary
=========

This document reports on the results of an automatic security scan.
The report first summarises the results found.
Then, for each host, the report describes every issue found.
Please consider the advice given in each description, in order to rectify
the issue.

All dates are displayed using the timezone "Coordinated Universal Time",
which is abbreviated "UTC".

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses
the actual threat of the result.

Notes are included in the report.Information on overrides is included in the report.

This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.

Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the
filtering described above. Before filtering there were 18 results.

Scan started: Fri Jan 24 02:11:50 2025 UTC
Scan ended: Fri Jan 24 03:02:39 2025 UTC
Task: Windows11

Host Summary
****

Host	High	Medium	Low	Log	False Positive
10.0.2.4	0	1	1	0	0
Total: 1	0	1	1	0	0

II Results per Host
===================

Host 10.0.2.4
****

Scanning of this host started at: Fri Jan 24 02:12:12 2025 UTC
Number of results: 2

Port Summary for Host 10.0.2.4

Service (Port)	Threat Level
135/tcp	Medium (CVSS: 5.0)
general/tcp	Low (CVSS: 2.6)

Security Issues for Host 10.0.2.4

Issue

NVT: DCE/RPC and MSRPC Services Enumeration Reporting
OID: 1.3.6.1.4.1.25623.1.0.10736
Threat: Medium (CVSS: 5.0)
Port: 135/tcp

Summary:

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC se!
rvices running
on the remote host can be enumerated by connecting on port 135 and doing the a!
ppropriate queries.

Vulnerability Detection Result:
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p!
rotocol:
Port: 49664/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: Ngc Pop Key Service
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: Ngc Pop Key Service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:10.0.2.4[49664]
Annotation: KeyIso
Port: 49665/tcp
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49665]
Port: 49666/tcp
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49666]
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49666]
Port: 49667/tcp
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49667]
Annotation: Windows Event Log
Port: 49668/tcp
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1

Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
Endpoint: ncacn_ip_tcp:10.0.2.4[49668]
Port: 49676/tcp
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:10.0.2.4[49676]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re!
porting this list is not enabled by default due to the possible large size of th!
is list. See the script preferences to enable this reporting.

Impact:
An attacker may use this fact to gain more knowledge
about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method:
Details:
DCE/RPC and MSRPC Services Enumeration Reporting
(OID: 1.3.6.1.4.1.25623.1.0.10736)
Version used: 2022-06-03T10:17:07Z

Issue

NVT: TCP Timestamps Information Disclosure
OID: 1.3.6.1.4.1.25623.1.0.80091
Threat: Low (CVSS: 2.6)
Port: general/tcp

Summary:
The remote host implements TCP timestamps and therefore allows
to compute the uptime.

Vulnerability Detection Result:
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4867830
Packet 2: 4869888

Impact:
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line
'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to appl!
y the settings at
runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timesta!
mps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be complete!
ly disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Tim!
estamp options when
initiating TCP connections, but use them if the TCP peer that is initiating co!
mmunication includes
them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS:
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight:
The remote host implements TCP timestamps, as defined by
RFC1323/RFC7323.

Vulnerability Detection Method:
Special IP packets are forged and sent with a little delay in
between to the target IP. The responses are searched for a timestamps. If foun!
d, the timestamps
are reported.
Details:
TCP Timestamps Information Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.80091)
Version used: 2023-12-15T16:10:08Z

References:
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url:
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.as
px?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090