Project 6: Vulnerability Scan

Cat's Vulnerability Scan

Prepared by: Esther Ogunlana
November 6, 2024

Executive Summary

This vulnerability assessment was conducted to evaluate potential security risks in Cat's company's network. The scan identified two notable vulnerabilities: one related to DCE/RPC and MSRPC Services Enumeration, which was categorized as Medium severity, and another related to TCP Timestamps Information Disclosure, which was categorized as Low severity. Although these vulnerabilities may not pose immediate critical risks, they could potentially be leveraged by attackers in combination with other weaknesses to gather sensitive information or launch more sophisticated attacks. Immediate action is recommended to mitigate these vulnerabilities and reduce the potential for an attack.

Scan Results

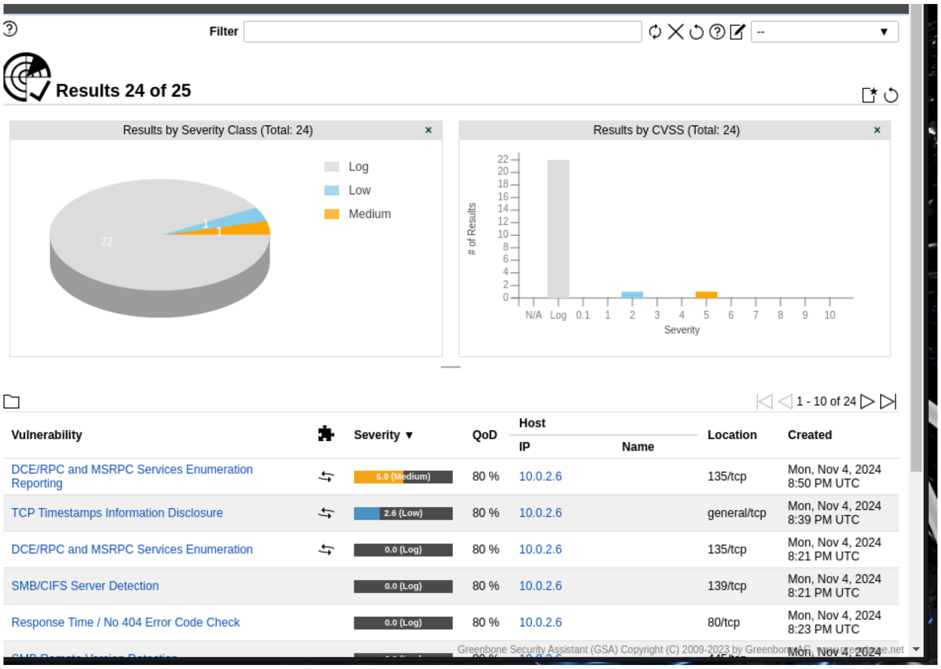
The vulnerability scan identified the following issues:

1. DCE/RPC and MSRPC Services Enumeration - Medium Severity
2. TCP Timestamps Information Disclosure - Low Severity

Both findings relate to information disclosure, which can provide attackers with valuable data for further exploitation.

The Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) protocol was developed to enable distributed software to operate as though it were running on a single system. One of its key features is service enumeration, which allows a client system to gather information about all the services running on a server (Haviland, 2023). Enabling this provides a gateway for threat actors to harvest information about our systems and services and this could be detrimental.

The TCP timestamp vulnerability on the other hand, is a security flaw that arises when a system's clock tracks time and multiple TCP packets are intercepted (Fortra, 2023). This weakness can be exploited to calculate the system's uptime, potentially revealing it as a target for an attack.


Filter
--
Results 24 of 25
Results by Severity Class (Total: 24)
22
1
1
Log
Low
Medium
Results by CVSS (Total: 24)
# of Results
22
20
18
16
14
12
10
8
6
4
2
0
N/A
Log
0.1
1
2
3
4
5
6
7
8
9
10
Severity
1 - 10 of 24
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.0.2.6		135/tcp	Mon, Nov 4, 2024 8:50 PM UTC
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	10.0.2.6		general/tcp	Mon, Nov 4, 2024 8:39 PM UTC
DCE/RPC and MSRPC Services Enumeration	⇆	0.0 (Log)	80 %	10.0.2.6		135/tcp	Mon, Nov 4, 2024 8:21 PM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	10.0.2.6		139/tcp	Mon, Nov 4, 2024 8:21 PM UTC
Response Time / No 404 Error Code Check		0.0 (Log)	80 %	10.0.2.6		80/tcp	Mon, Nov 4, 2024 8:23 PM UTC

Figure 1: Screenshot Showing Scan Result of the Windows 11 Machine

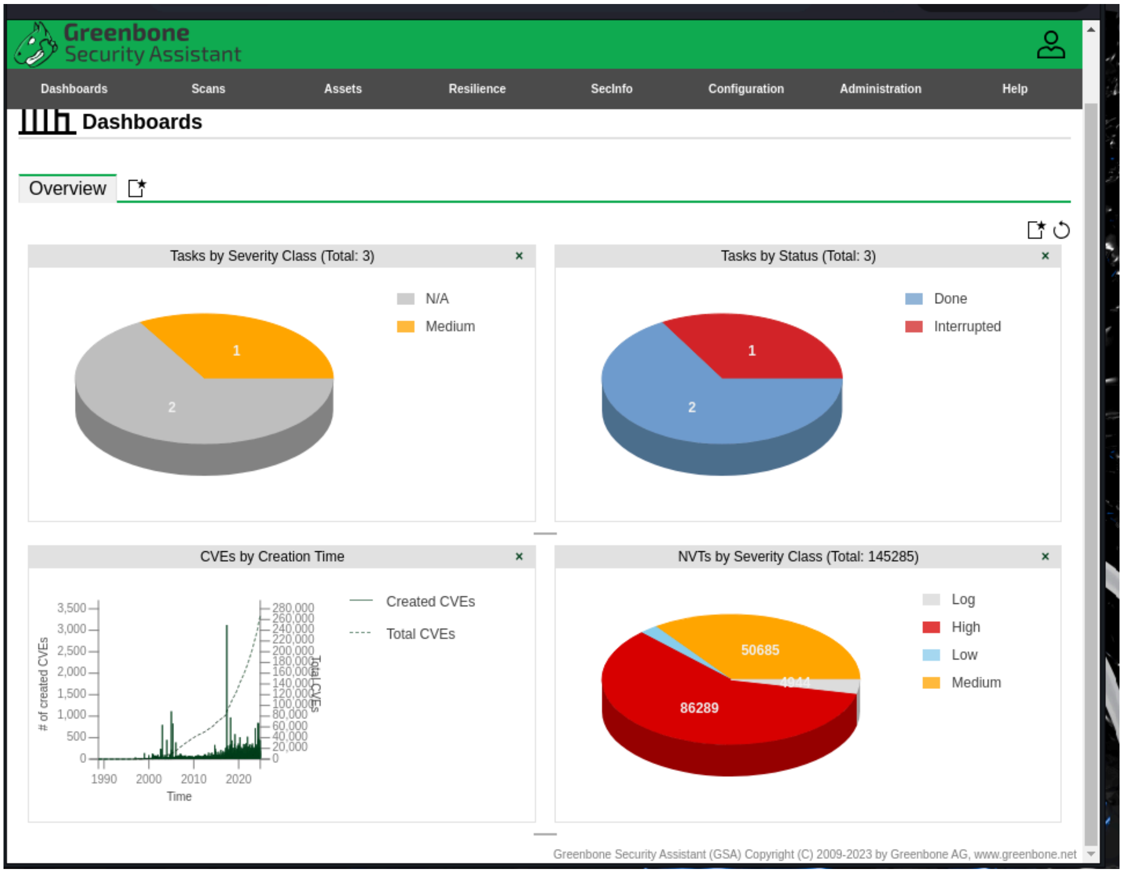


Figure 2: Screenshot Showing the Overview of Scans Performed

Methodology

Vulnerability Assessment Platform

The vulnerability scan was carried out using OpenVAS, a comprehensive vulnerability scanner that offers a wide range of features. It supports unauthenticated and authenticated testing, can assess various high-level and low-level internet and industrial protocols, includes performance optimization for large-scale scans, and provides a robust internal programming language for customizing and implementing any type of vulnerability test (Greenbone, n.d).

Findings

DCE/RPC and MSRPC Services Enumeration (Medium Severity)

Description: DCE/RPC and MSRPC are protocols used by Windows operating systems for remote communication between systems. When improperly configured, these services may disclose information about the operating system, installed software, and network configuration. This information can be valuable to attackers, as it can aid in identifying potential vulnerabilities or misconfigurations in the system.

Impact: The disclosure of service details (such as the version of MSRPC or DCE/RPC services) can allow attackers to:

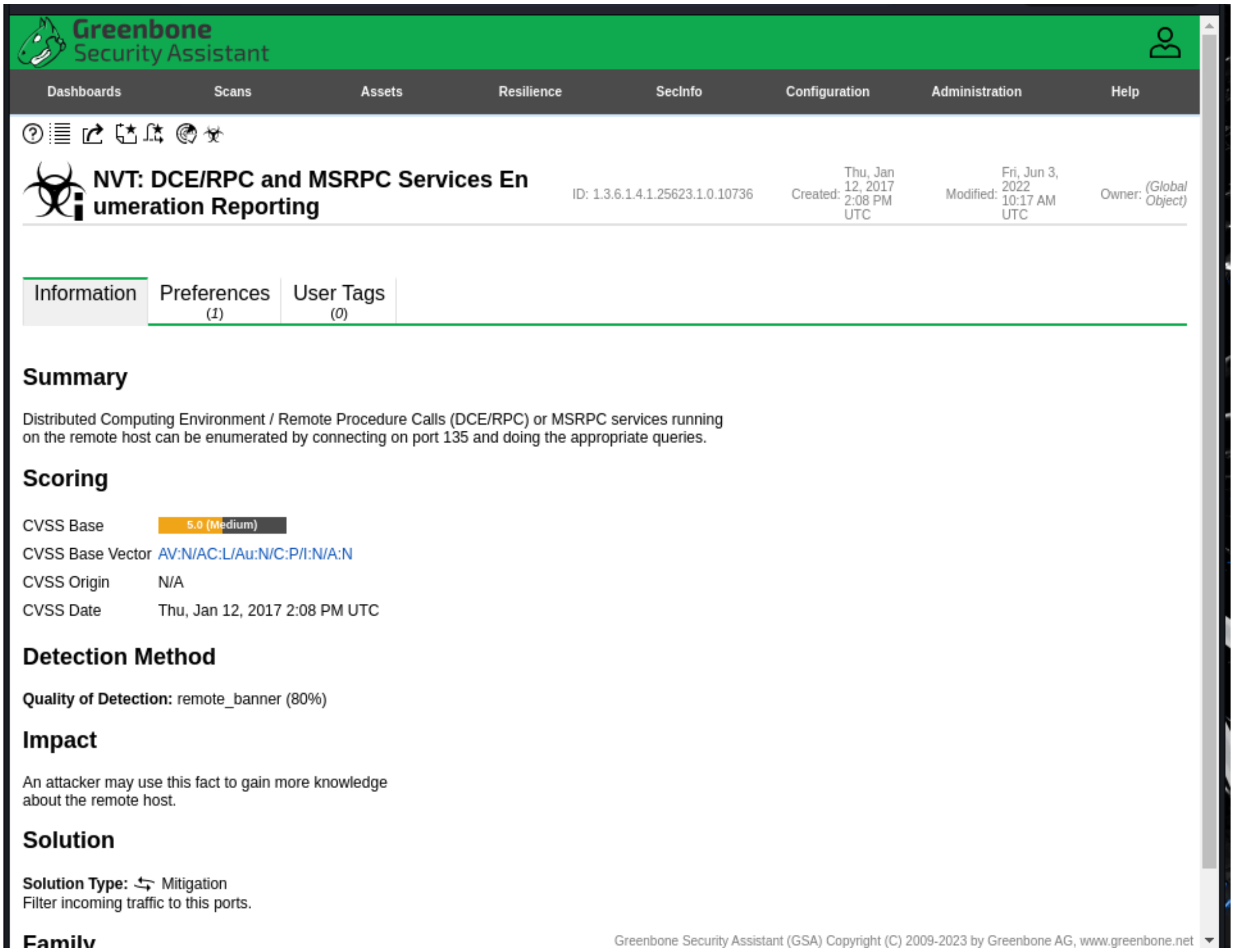
Gather information on the operating system version.

Identify potential vulnerabilities in specific services.

Map out the network topology.

Potential Risk: An attacker could use this information to target specific vulnerabilities in the identified services (e.g., exploiting known vulnerabilities in MSRPC). While not directly exploitable, this enumeration could act as reconnaissance that aids in further attacks.

Solution: To mitigate this, disable unnecessary services such as DCE/RPC and MSRPC on systems that do not require them. Use firewall rules to limit exposure of these services to trusted internal systems and networks.



NVT: DCE/RPC and MSRPC Services Enumeration Reporting

ID: 1.3.6.1.4.1.25623.1.0.10736 Created: Thu, Jan 12, 2017 2:08 PM UTC Modified: Fri, Jun 3, 2022 10:17 AM UTC Owner: *(Global Object)*

Summary

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.

Scoring

CVSS Base	5.0 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Origin	N/A
CVSS Date	Thu, Jan 12, 2017 2:08 PM UTC

Detection Method

Quality of Detection: remote_banner (80%)

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.

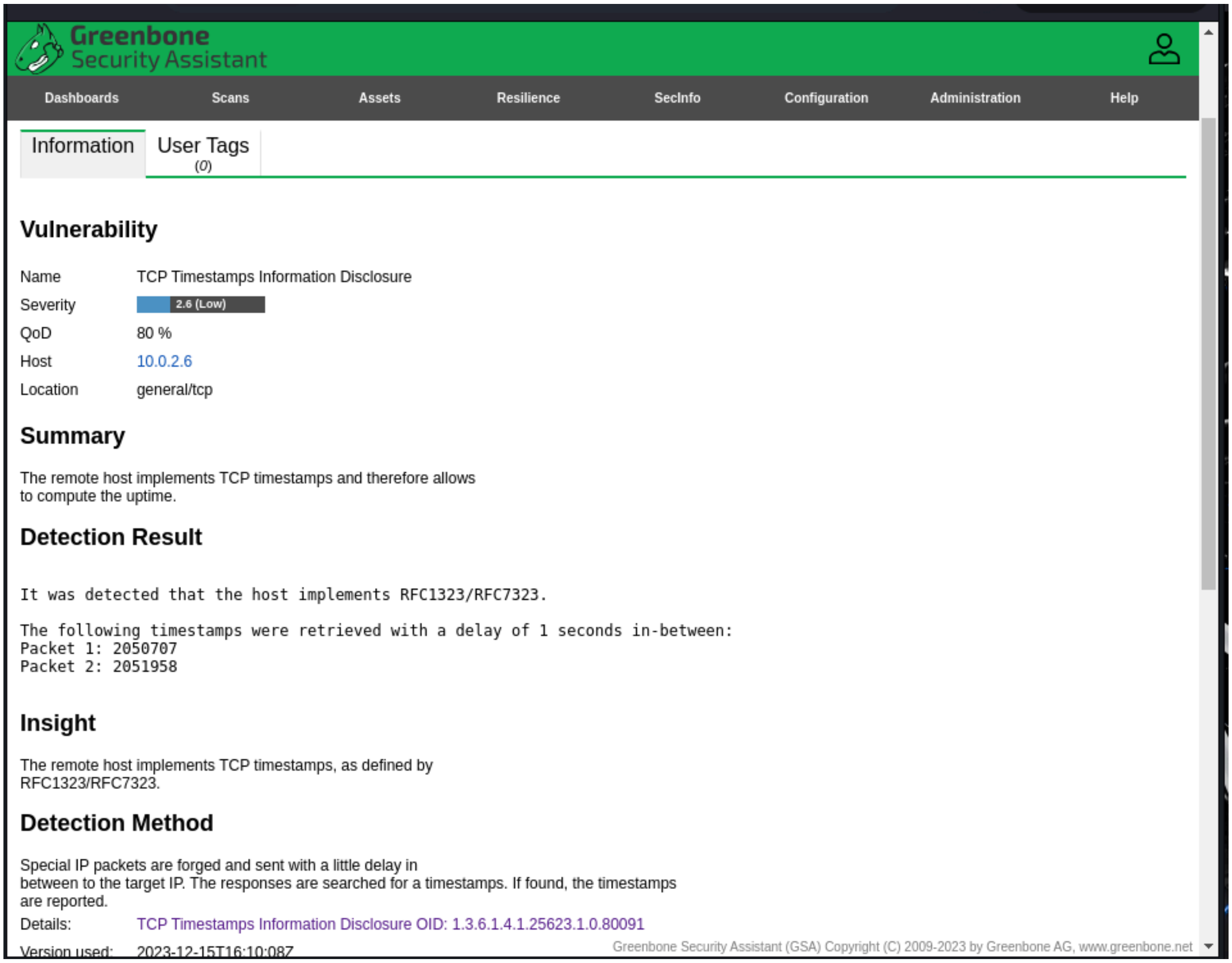
Family

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Figure 3: Screenshot Showing DCE/RPC and MSRPC Vulnerability.

TCP Timestamps Information Disclosure (Low Severity)

Description: The TCP timestamp option is used by certain operating systems to help calculate round-trip time for network communication. This timestamp can be exposed as part of a network packet and may allow attackers to infer details about the system's uptime and potentially deduce information about the internal network structure.
Impact: By analyzing the TCP timestamps, an attacker can estimate:
The system’s uptime and potentially gain insight into the system's reboot cycles.
The time zone or geographical location of the system based on timestamp patterns.
Potential Risk: While this vulnerability is typically not critical, it may provide an attacker with valuable intelligence for other forms of attack (e.g., social engineering or denial of service attacks). While it is generally considered a low-risk vulnerability, it still contributes to an attacker's ability to gather information passively.
Solution: Disable TCP timestamps where they are not required. This can be done at the OS level (e.g., configuring the firewall to block timestamp requests or adjusting TCP/IP stack settings to not reply with timestamps).



Vulnerability

Name	TCP Timestamps Information Disclosure
Severity	2.6 (Low)
QoD	80 %
Host	10.0.2.6
Location	general/tcp

Summary

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

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: 2050707
Packet 2: 2051958
```

Insight

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

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 found, 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

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Figure 4: Screenshot Showing TCP Timestamp Vulnerability Report

Risk Assessment

Vulnerability	Severity	Description	Impacted Service/System	Potential Impact	Solution
DCE/RPC and MSRPC Services Enumeration	Medium	Information disclosure via MSRPC/DCE/RPC services, revealing OS and service details.	Networked Windows systems	Potential reconnaissance for further exploitation.	Disable unnecessary services, and restrict with firewall rules.
TCP Timestamps Information Disclosure	Low	Information disclosure via TCP timestamps, revealing system uptime and time-based data.	Networked systems with open ports	Minor intelligence gain for attackers.	Disable TCP timestamps at the OS level.

Recommendations

Mitigation of DCE/RPC and MSRPC Enumeration:

Prioritize Disabling Unnecessary Services: Any systems that do not require DCE/RPC or MSRPC should have these services disabled to reduce exposure. For systems that must run these services, restrict access to trusted hosts via firewalls.
Audit Service Configurations: Regularly audit and ensure that only necessary services are running on systems. For example, MSRPC should be restricted to internal network communication and not exposed to external-facing systems.
Vulnerability Management: Regularly patch any services related to DCE/RPC or MSRPC to mitigate vulnerabilities that could be exploited once this information is gathered.
Mitigation of TCP Timestamp Disclosure:

Disable TCP Timestamping: On all systems where uptime is not a necessary detail to be exposed, disable TCP timestamps through system configurations or firewall rules. This can be accomplished through OS-level configurations, such as adjusting TCP/IP stack settings in Linux (e.g., setting timestamp to 0 in /proc/sys/net/ipv4/tcp_timestamps).
Network Segmentation: Ensure that exposed services, especially those that may respond with TCP timestamps, are appropriately segmented from the broader network to limit exposure to external attackers.

Conclusion

The vulnerabilities identified in this report (DCE/RPC and MSRPC Services Enumeration and TCP Timestamps Information Disclosure) pose a moderate risk to Cat's company’s security posture. While neither vulnerability is highly critical, they provide attackers with valuable information that could facilitate more targeted attacks. By disabling unnecessary services and securing network communications (including disabling TCP timestamps), Cat’s company can significantly reduce the potential attack surface and strengthen its defenses against future exploits.

References

CVE Details: Common Vulnerabilities and Exposures (CVE). https://www.cve.org/

Fortra. (2023, September 15). *TCP timestamp response vulnerability fix*. Beyond Security. https://www.beyondsecurity.com/resources/vulnerabilities/tcp-timestamps-retrieval#:~:text=Vulnerabilities%20in%20TCP%20Timestamps%20Retrieval%20is%20a%20Low%20risk%20vulnerability,CVSS%20Score:

Greenbone openvas. OpenVAS. (n.d.). https://www.openvas.org/

Haviland, J. (2023, December 6). *The risks of DCE/RPC service enumeration*. Critical Path Security. https://www.criticalpathsecurity.com/the-risks-of-dce-rpc-service-enumeration/

National Institute of Standards and Technology (NIST), SP 800-53: *Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

National Vulnerability Database (NVD), CVE-2023-XXXX: *DCE/RPC Enumeration*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53.pdf