Project 6 Cat's Company Vulnerabilities Report

Executive Summary

The vulnerability assessment scans conducted on the company's IT infrastructure using the "Greenbone" application have provided valuable insights into the security posture of the organization. These scans have identified vulnerabilities that, if left unaddressed, could be exploited by cybercriminals to gain unauthorized access, compromise systems, and compromise the integrity of critical data. The purpose of this report is to outline the results of the scans, recommend the top six vulnerabilities that should be prioritized for mitigation, propose potential mitigations for each vulnerability, and provide a rationale behind these recommendations.

The vulnerability scans targeted three devices within the company's network: a Windows workstation, a Windows server, and a Linux system. These scans revealed a range of vulnerabilities across the systems, highlighting potential weaknesses that cybercriminals could exploit. It is essential for the organization to address these vulnerabilities promptly to minimize the risk of unauthorized access, data breaches, and other detrimental cyber threats that could disrupt business operations.

Scan results

Based on the scan results, six vulnerabilities have been identified as the most critical and should be prioritized for mitigation. The prioritization of these vulnerabilities is based on their potential impact, exploitability, and the level of risk they pose to the organization. Critical vulnerabilities demanding immediate attention have been ranked at the top, considering their severe consequences on system integrity and confidentiality. High and medium vulnerabilities have also been included due to their potential to compromise security and expose sensitive information. While low-severity vulnerabilities may have a lower impact, addressing them contributes to maintaining system availability and overall security posture.

Methodology

To conduct the vulnerability assessment scans, the following tools and tests were utilized:

1. Kali Linux with GVM (Greenbone Vulnerability Management): Kali Linux is a specialized Linux distribution that includes various security tools, including GVM. GVM is an open-source framework that incorporates the Greenbone

vulnerability scanning tool. GVM was installed and used within the Kali Linux environment for vulnerability scanning and assessment purposes.

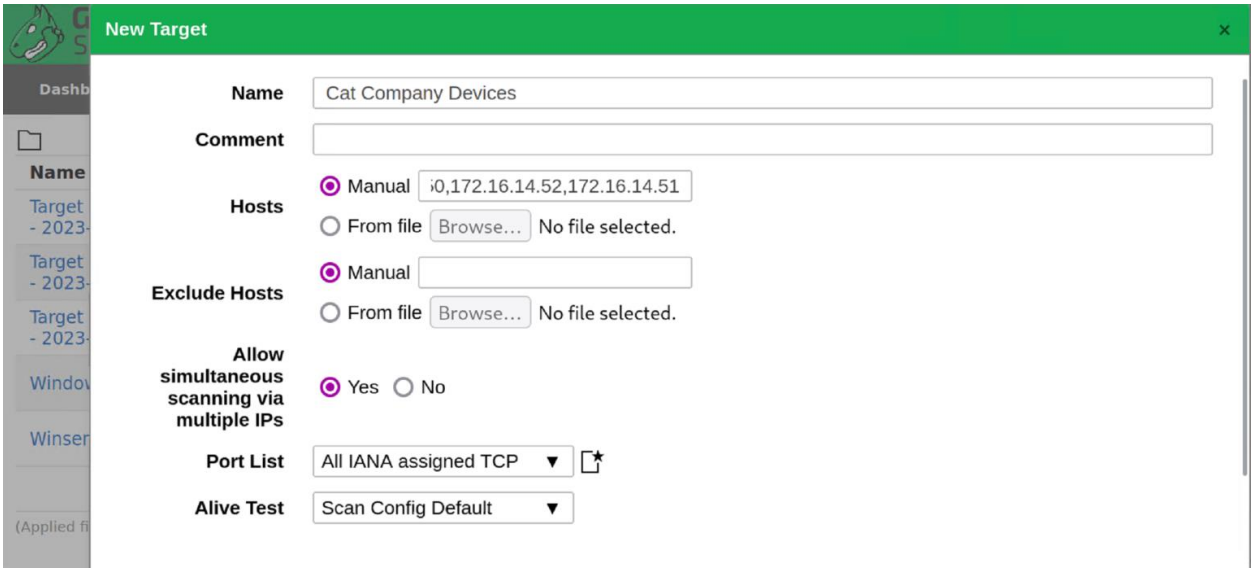
2. Greenbone: Greenbone is a vulnerability management solution that provides comprehensive vulnerability scanning capabilities. It uses a database of known vulnerabilities and performs various tests to identify weaknesses within the target systems. Greenbone was utilized to scan and assess the vulnerabilities present in the company's IT infrastructure. (Feilner & Zurborn, 2023)

Environment and Target Setup

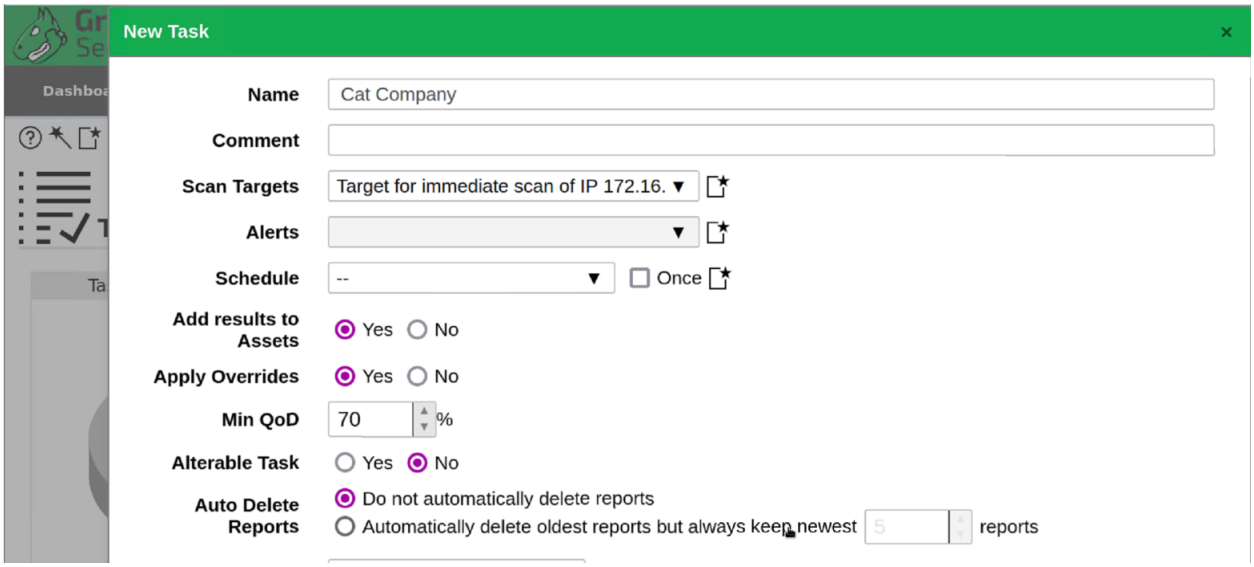
The vulnerability assessment scans were performed in the EVE (Emulated Virtual Environment) lab environment, utilizing a KaliOpenVAS device. This device was configured with the Kali Linux operating system and had GVM (Greenbone Vulnerability Management) software installed on it.

To create the target and tasks for the scans, the following steps were followed:

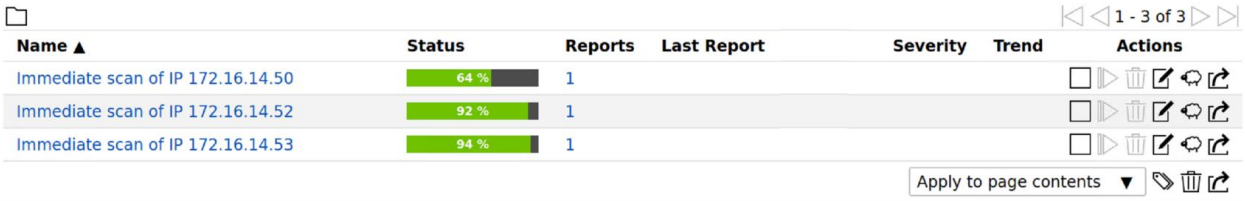
1. Target Creation: Within the Greenbone interface on the KaliOpenVAS device, the target devices in the company's network were defined and added to the scan. This included the Windows workstation, the Windows server, and the Linux system.



2. Task Creation: After defining the target devices, tasks were created within the Greenbone interface to specify the type of scans and tests to be performed on each target. The purpose of each scan and test was determined based on the desired objectives, such as identifying vulnerabilities, assessing risk levels, and providing essential information for decision-making and preparations.



3. Scan Execution: Once the targets and tasks were set up, the scans were initiated within the Greenbone interface. Greenbone performed the scans by utilizing various scanning techniques, including port scanning and vulnerability scanning, to identify potential vulnerabilities within the target systems.



The results obtained from the scans were collected and used for further evaluation and analysis to determine the vulnerabilities present and prioritize mitigation efforts.

Findings

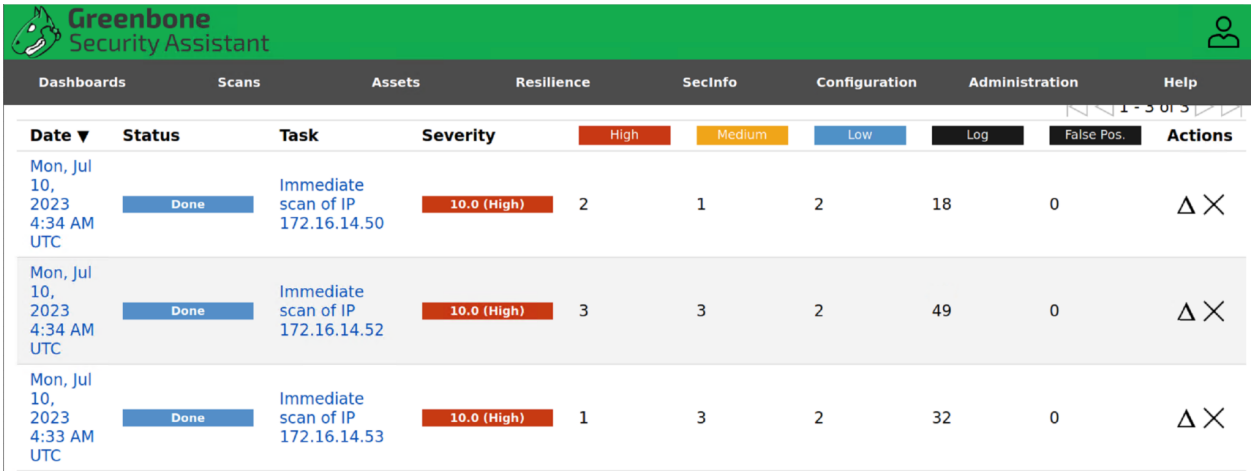
The vulnerability assessment scans were conducted successfully on all targeted systems within the company's network. A total of 11 vulnerabilities were identified across the 3 targets. It is crucial to prioritize these vulnerabilities based on their severity levels to effectively manage the large number of identified vulnerabilities.

The severity levels of the vulnerabilities varied across the targets, with all 3 targets having 10.0 severity level.

Prioritizing vulnerabilities is essential for efficient resource allocation and risk management. Without prioritization, organizations may end up allocating resources to address lower-risk vulnerabilities while higher-risk vulnerabilities remain

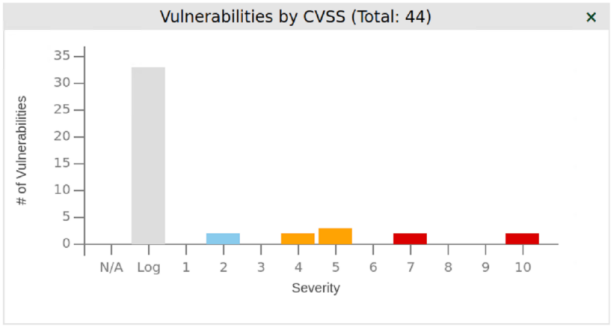
unaddressed, leaving critical systems and data exposed to potential cyber threats. (Mukherjee, 2023)

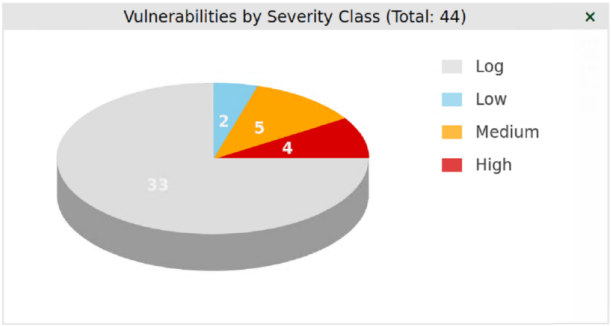
The Linux machine (IP address: 172.16.14.52), Windows 1 (IP address: 172.16.14.50), and Winserver (IP address: 172.16.14.53) were all successfully scanned, allowing for a comprehensive assessment of their vulnerabilities.



Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Mon, Jul 10, 2023 4:34 AM UTC	Done	Immediate scan of IP 172.16.14.50	10.0 (High)	2	1	2	18	0	
Mon, Jul 10, 2023 4:34 AM UTC	Done	Immediate scan of IP 172.16.14.52	10.0 (High)	3	3	2	49	0	
Mon, Jul 10, 2023 4:33 AM UTC	Done	Immediate scan of IP 172.16.14.53	10.0 (High)	1	3	2	32	0	

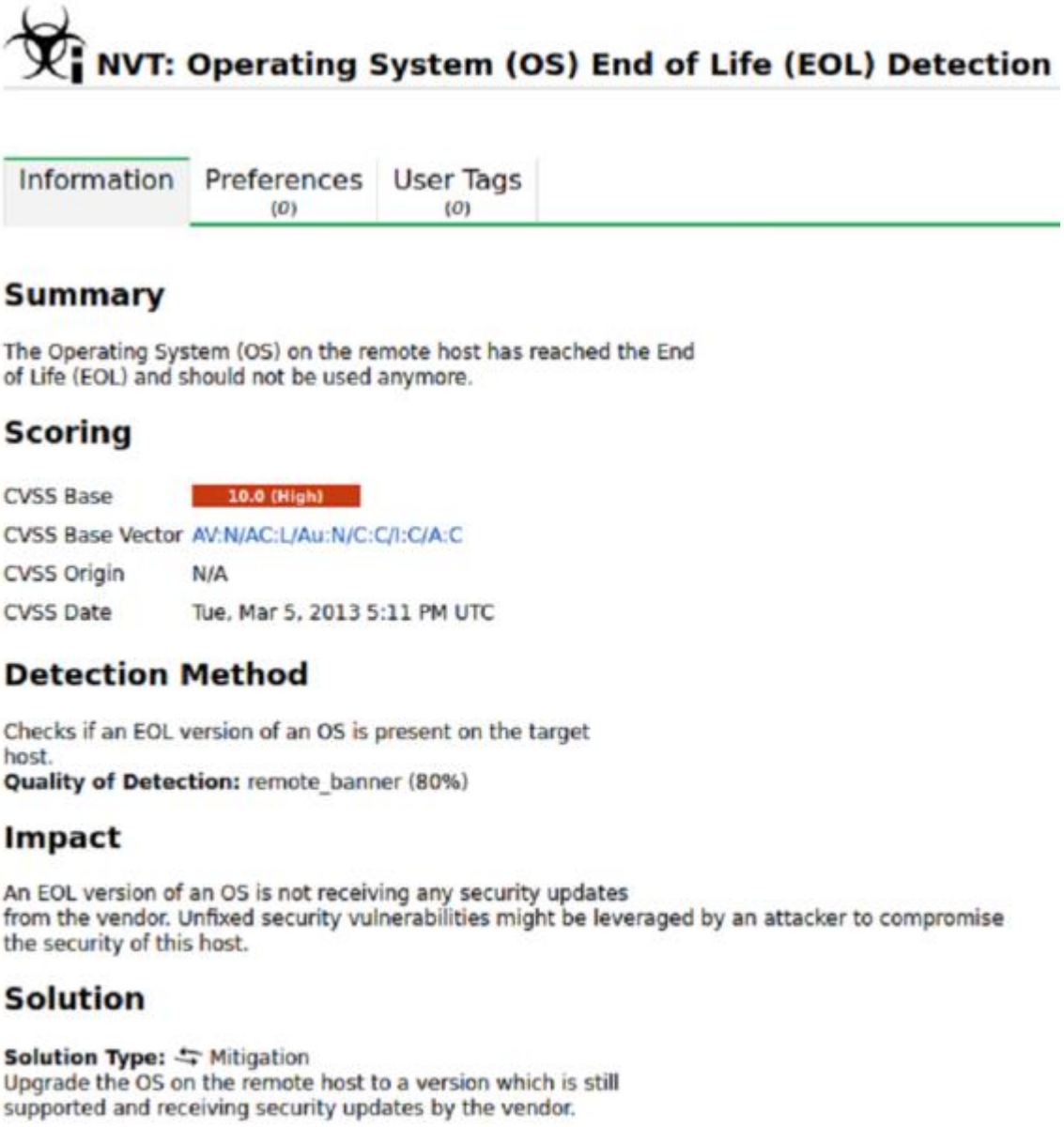
The scan gave more information on vulnerabilities present based on severity levels.





Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Report outdated / end-of-life Scan Engine / Environment (local)	Mon, Jul 10, 2023 4:36 AM UTC	Mon, Jul 10, 2023 4:37 AM UTC	10.0 (High)	97 %	3	3
Operating System (OS) End of Life (EOL) Detection	Mon, Jul 10, 2023 4:44 AM UTC	Mon, Jul 10, 2023 4:44 AM UTC	10.0 (High)	80 %	1	1
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)	Mon, Jul 10, 2023 4:39 AM UTC	Mon, Jul 10, 2023 4:39 AM UTC	7.5 (High)	80 %	1	1
HTTP Brute Force Logins With Default Credentials Reporting	Mon, Jul 10, 2023 4:46 AM UTC	Mon, Jul 10, 2023 4:46 AM UTC	7.5 (High)	95 %	1	1
SSL/TLS: Report Weak Cipher Suites	Mon, Jul 10, 2023 4:42 AM UTC	Mon, Jul 10, 2023 4:42 AM UTC	5.0 (Medium)	98 %	1	1
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Mon, Jul 10, 2023 4:45 AM UTC	Mon, Jul 10, 2023 4:45 AM UTC	5.0 (Medium)	70 %	1	1
DCE/RPC and MSRPC Services Enumeration Reporting	Mon, Jul 10, 2023 4:44 AM UTC	Mon, Jul 10, 2023 4:45 AM UTC	5.0 (Medium)	80 %	9	2
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	Mon, Jul 10, 2023 4:42 AM UTC	Mon, Jul 10, 2023 4:42 AM UTC	4.3 (Medium)	98 %	1	1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	Mon, Jul 10, 2023 4:42 AM UTC	Mon, Jul 10, 2023 4:42 AM UTC	4.0 (Medium)	80 %	2	1
TCP Timestamps Information Disclosure	Mon, Jul 10, 2023 4:41 AM UTC	Mon, Jul 10, 2023 4:44 AM UTC	2.6 (Low)	80 %	3	3

The findings from the vulnerability assessment scans were compiled into a comprehensive report, which included detailed information about each vulnerability, recommended mitigation measures, and suggestions for improving security configurations and policies. This allowed Cat's Company to address vulnerabilities promptly and enhance its overall security posture. By utilizing Greenbone's vulnerability management tool, the company gained valuable insights into its systems and received guidance on necessary patches and protective measures. This proactive approach to vulnerability management ensures that Cat's Company remains resilient against potential cyber threats and can make informed decisions to mitigate risks effectively.



Another SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094):

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Scoring

CVSS Base	5.0 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Origin	N/A
CVSS Date	Fri, Oct 29, 2021 8:24 AM UTC

Insight

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Quality of Detection: remote_analysis (70%)

Affected Software/OS

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Impact

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution

Solution Type: Vendorfix
Users should contact their vendors for specific patch information.

Risk Assessment

The vulnerability assessment scans conducted on the targeted systems revealed a total of 11 vulnerabilities across the Linux machine, Windows 1, and Winserver.

Among these vulnerabilities, there were 2 categorized as Low severity, 5 as Medium severity, and 4 as High severity.

Below is a table summarizing the vulnerabilities, their impact, severity, and recommended fixes:

HIGH

Machine	**Vulnerabilities**	**Impact**	**Severity**	**Fix**
Windows 1 (Windows 10 Pro 1507) 172.16.14.50	OS End of life (EOL) detection EOL Date 2017-05-09	OS -Not receiving any security update from vendor. Unfixed security vulnerabilities	10.0	Mitigation Upgrade the OS
Linux Machine 172.16.14.52	Unprotected OSSEC/Wazuh Ossec-authd	Misused by a remote attacker to register arbitrary agents at the remote service or overwrite the registration of existing ones taking them out of service	7.5	Workaround Enable password authentication or client certificate verification within the config of ossec-authd
Linux Machine 172.16.14.52	HTTP Brute Force logins with default credentials reporting	The issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration	7.5	Mitigation Change the password ASAP

Medium: These have moderate risk and lesser impact as compared to high vuln but should still be addressed.

Machine	Vulnerabilities	Impact	Severity	Fix
Linux Machine 172.16.14.52	SS/TLS: Renegotiation DoS Vulnerability (CVE.2011-1473, CVE-2011-5094)	The flaw might make it easier remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection	5.0	Vendorfix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SS/TLS service.
Winserver 172.16.14.53	SSL/TLS: Report Weak Cipher Suites	RC4 is considered to be weak (CVE-2013-2566,CVE-2015-2808) Ciphers using 64 bit or less are considered to be vulnerable to brute force and therefore considered as weak (CVE-2015-4000) 1024 bit RSA authentication is considered to be insecure and therefore as weak	5.0	Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Windows1 172.16.14.50 And	DCE/RPC and MSRPC Serves Enumeration Reporting	An attacker may use this fact to gain more knowledge	5.0	Mitigation Filter incoming traffic to this ports

Winserver 172.16.14.53		about the remote host.		
Linux Machine 172.16.14.52	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	An attacker might able to decrypt the SS/TLS communication offline.	4.0	Workaround Deploy (Ephemeral) Elliptic-Curve Diffe-Hellman (ECDHE) or use a 2048 or stronger Diffe-Hellman group. For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Low: Although they may not require immediate attention, addressing them should be ensured.

Machine	**Vulnerabilities**	**Impact**	**Severity**	**Fix**
Windows1 172.16.14.50, Winserver 172.16.14.53, Linux Machine 172.16.14.52	TCP Timestamps information disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed	2.6	Mitigation To disable TCP timestamps on linux add the line 'net.ipv4tcp timestamps – O' to 'etctsysctl.conf. Execute •sysctl

				-p' to apply the settings at runtime.
Windows1 172.16.14.50, Winserver 172.16.14.53, Linux Machine 172.16.14.52	ICMP Timestamp Reply information disclosure	The information could theoretically be used to exploit weak time-based random number generators in other services	2.1	Mitigation - Disable support for ICMP timestamp the remote host completely - Protect the remote host by a firewall. and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Recommendations

Based on the identified vulnerabilities and their severity levels, the following actions should be taken in a prioritized order:

1. Mitigate High Severity Vulnerabilities: a. Windows 1 (Windows 10 Pro 1507) - OS End of Life (EOL) detection:

- Mitigation: Upgrade the operating system to a supported version. The EOL status indicates that the OS is not receiving security updates, leaving it vulnerable to exploitation. Upgrading to a supported version ensures continued security patches and mitigates the risk of potential attacks.

b. Linux Machine - Unprotected OSSEC/Wazuh Ossec-authd:

- Mitigation: Enable password authentication or client certificate verification within the configuration of ossec-authd. This prevents remote attackers from registering arbitrary agents or overwriting existing registrations, safeguarding the availability and integrity of the OSSEC/Wazuh service.

2. Address Medium Severity Vulnerabilities: a. Linux Machine - SS/TLS: Renegotiation DoS Vulnerability:

- Mitigation: Contact the vendor for specific patch information or remove/disable renegotiation capabilities altogether from the affected SS/TLS service. This helps prevent potential Denial of Service (DoS) attacks resulting from excessive renegotiations.

b. Winserver - SSL/TLS: Report Weak Cipher Suites:

- Mitigation: Change the server's configuration to not accept weak cipher suites. By disallowing vulnerable cipher suites like RC4 and 1024-bit RSA authentication, the server's resistance against brute force attacks is improved, enhancing the confidentiality of SSL/TLS communications.

c. Windows 1 and Winserver - DCE/RPC and MSRPC Serves Enumeration Reporting:

- Mitigation: Implement filtering rules to restrict incoming traffic to the corresponding ports. This helps prevent unauthorized individuals from gaining excessive knowledge about the remote hosts and mitigates the risk of potential attacks leveraging this information.

3. Mitigate Low Severity Vulnerabilities: a. Windows 1, Winserver, and Linux Machine - TCP Timestamps information disclosure:

- Mitigation: Disable TCP timestamps on the respective systems by modifying the 'etctsysctl.conf' file and applying the settings at runtime. Disabling TCP timestamps prevents the computation of system uptime, reducing the potential for information disclosure.

b. Windows 1, Winserver, and Linux Machine - ICMP Timestamp Reply information disclosure:

- Mitigation: Disable support for ICMP timestamp completely or block ICMP packets passing through the firewall. By preventing the disclosure of timestamp information, the risk of exploiting weak time-based random number generators in other services is minimized.

c. Linux Machine - SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability:

- Workaround: Deploy (Ephemeral) Elliptic-Curve Diffe-Hellman (ECDHE) or use a 2048 or stronger Diffie-Hellman group. By implementing stronger Diffie-Hellman parameters, the risk of offline decryption of SSL/TLS communication is reduced.

By following these recommendations, Cat's Company can effectively address the identified vulnerabilities, strengthen its security posture, and minimize the risk of unauthorized access, data breaches, and potential disruptions to critical operations.

References

Feilner, M., & Zurborn, B. (2023, July 7). *Vulnerability management: Open source und DSGVO-Konform*. Greenbone. https://www.greenbone.net/

Mukherjee, A. (2023, April 10). *Prioritizing vulnerabilities : A risk based approach*. Prioritizing Vulnerabilities : A Risk Based Approach. https://www.threatintelligence.com/blog/vulnerability-prioritization