Cat’s Company Vulnerabilities Project

By Heather Fincati

March 11, 2024

Table of Contents

1. Executive Summary

A vulnerability scan of our network revealed concerning security issues on the Linux system, while the Winserver showed no vulnerabilities (possibly due to an outdated scanner). The Linux machine has critical, high, and medium severity vulnerabilities that need immediate attention. These include unprotected services, weak password configurations, and outdated protocols.

To address these issues, we recommend updating the scan engine on all machines, enabling password protection for vulnerable services on Linux, patching software and updating encryption technology that secures data transmitted between the website and users configurations, and potentially disabling weak protocols and functionalities. We should also implement a vulnerability management policy and implement a Zero Trust Security Model to improve our overall security posture.

2. Scan Results

We successfully scanned all three target systems. Our scans revealed a mix of vulnerabilities, with three critical severity, two high severity, two medium severity and 2 low severity vulnerabilities. I have provided further information about each in the Risk Management section of this report. The raw scan results can be found in the appendices (A, B, C).

3. Methodology

Tools and Tests

- OpenVAS Greenbone (Scanner):
    - **Purpose:** OpenVAS Greenbone is a full-featured vulnerability scanner. It performs various vulnerability tests against the target system, identifying potential security weaknesses.
    - **Environment:** OpenVAS Greenbone was installed and executed on a dedicated Kali Linux machine.

Data Sources

- CVE Database:
    - **Purpose:** The Common Vulnerabilities and Exposures (CVE) database provides a catalog of publicly known security vulnerabilities. OpenVAS leverages the CVE database to identify relevant tests for the target system.
    - **Environment:** The CVE database is an online resource accessible through the internet.

4. Findings

The vulnerability scan results are encouraging for the Winserver, which showed no security weaknesses. However, this might be due to a few possibilities; Outdated GVM scanner, misconfiguration issue with the GVM, or truly the Winserver is free from exploitable vulnerabilities. As the report highlights, the scan engine might not be up-to-date. While the Winserver results are positive, further investigation is needed to confirm the cause. The Linux system, on the other hand, did show vulnerabilities that require immediate attention.

5. Risk Assessment

This report identifies security risks that could have significant impact on day-to-day business operations and client interactions.

Critical Severity	High Severity	Medium Severity	Low Severity
3	2	2	2

Critical Severity Vulnerability

Three of the vulnerabilities that came up in the scan were critical. They were due to the outdated scan engine on each machine. While not an actual vulnerability in-and-of itself, this leaves the systems vulnerable to exploits not covered by the outdated scan engine.

High Severity Vulnerabilities

The scan came back with 2 unique vulnerabilities with high severity. High severity vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

A table of the high severity vulnerabilities is below:

Vulnerability	Description	Remediation	CVSS Score	Affected Machine
Unprotected OSSEC [1]	The remote service is not protected by; password authentication or client certificate verification.	Enable password authentication or client certificate verification.	7.5(High)	Linux
CVE-1999-0508 HTTP Brute Force [2]	An account on a router, firewall, or other network device has a default, null, blank, or missing password.	Updating the software and password complexity requirements, such as minimum length and including a combination of uppercase letters, lowercase letters, numbers, and special characters. Also, ensure default passwords are changed immediately upon deployment.	7.5(High)	Linux

Medium Severity Vulnerabilities

2 unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

A Table of the Medium Severity vulnerabilities is provided below:

Vulnerability	Description	Remediation	CVSS Score	Affected Machine
CVE-2011-5094 3 SSL/TLS Renegotiation DoS	Flaw in SSL/TLS service allows client-initiated renegotiation.	Disable renegotiation capabilities from affected service.	5.0 (medium) **	Linux
CVE-2015-0204 4 SSL/TLS: Depreciated TLSv1.0 and TLSv1.1 Protocol Detected	Attackers can eavesdrop on connections using deprecated protocols.	Disable TLSv1.0 and/or TLSv1.1 or upgrade Java.	4.3 (Medium) **	Windows1

***NOTE: These Vulnerabilities have been modified since last analyzed by the NVD (NVD, 2015). They are awaiting reanalysis which may result in further changes to the information provided. Therefore does not have a base score, due to this we have left it in Medium until further notice.*

Low Severity Vulnerabilities

2 unique low severity vulnerabilities were found in the initial scan. After further research right now.

A table of the Low Severity Vulnerabilities is provided below:

Vulnerability	Description	Remediation	CVSS Score	Affected Machine
CVE-2019-18625[6] TCP Timestamps Information Disclosure	Uptime of the remote host can be revealed.	Disable TCP timestamps	2.6(Low)	Linux
CVE-1999-0524 [7] ICMP Timestamp Reply	Information disclosure could be used to exploit weak RNG.	Disable ICMP timestamps and implement firewall rules blocking ICMP packets.	2.1(Low)	Linux

6. Recommendations

1. Address Critical-Severity Vulnerabilities

Reasoning: The outdated scan engine leaves the systems vulnerable to exploits not detected by the current version. This is the most critical issue because it undermines the effectiveness of future vulnerability scans.

Action:

Update the vulnerability scan engine on all machines (Linux, Windows1, and Winserver).

2. Address High-Severity Vulnerabilities

Reasoning: High-severity vulnerabilities are easier to exploit and can grant attackers significant access to the system.

Actions:

Unprotected OSSEC (Linux Machine): Enable password authentication or client certificate verification for OSSEC.

CVE-1999-0508 (Linux Machine): Update the software on the router, firewall, or network device to address the default password issue. Updating the software and password complexity requirements, such as minimum length and including a combination of uppercase letters, lowercase letters, numbers, and special characters. Also, ensure default passwords are changed immediately upon deployment and require users to create unique, strong passwords.

3. Address Medium-Severity Vulnerabilities

Reasoning: While less critical than high-severity vulnerabilities, these can still provide attackers with valuable information for future attacks.

Actions:

CVE-2011-5094 (Linux Machine): Contact the vendor of the software using the vulnerable SSL/TLS library (NSS) for specific patch information. Alternatively, disable renegotiation capabilities altogether.

CVE-2015-0204 (Windows1 Machine): Disable the deprecated TLSv1.0 and TLSv1.1 protocols on the affected system and enable TLSv1.2 or later versions.

4. Address Low-Severity Vulnerabilities

Reasoning: These vulnerabilities are the least critical but can still be exploited under specific circumstances.

Actions:

CVE-2019-18625 (Linux Machine): Consider disabling TCP timestamps on Linux by adding the line net.ipv4.tcp_timestamps = 0 to /etc/sysctl.conf and running sysctl -p to apply the changes. Evaluate the potential impact on other functionalities before implementing this change.

CVE-1999-0524 (Linux Machine): Evaluate the possibility of disabling ICMP timestamp support on the affected system. Alternatively, consider implementing firewall rules to block ICMP packets from untrusted networks.

Security Policy Recommendations

- Implement a vulnerability management policy that mandates regular scans and timely patching of vulnerabilities based on their severity.
- Implementation of a Zero Trust Security Model would increase an organization’s cyber security posture for today's digital transformation (Government of Canada, 2022)[8]
- Keep all software on systems up-to-date, including the vulnerability scanning tool.
- Consider implementing a web application firewall (WAF) to provide additional protection against web-based attacks.

7.Citations

1: Security Space, Vulnerability Scan, Published: November 9, 2017
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108547

2: CVE - CVE-1999-0508, CVE
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0508

3: NVD - CVE-2011-5094, NVD, Published: June 16, 2012
https://nvd.nist.gov/vuln/detail/CVE-2011-5094

4: NVD - CVE-2015-0204, NVD, Published: January 8, 2015
https://nvd.nist.gov/vuln/detail/CVE-2015-0204

5: NVD - CVE-2022-40735, NVD, Published: November 14, 2022
https://nvd.nist.gov/vuln/detail/CVE-2022-40735

6: NVD - CVE-2019-18625, NVD, Last Modified: February 01, 2023
https://nvd.nist.gov/vuln/detail/CVE-2019-18625

7: NVD - CVE-1999-0524, NVD last modified: November 14, 2022
https://nvd.nist.gov/vuln/detail/CVE-1999-0524

8: Zero Trust security model - ITSAP.10.008, Canadian Centre for Cyber Security, Published: November 2022
https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008

Appendix A

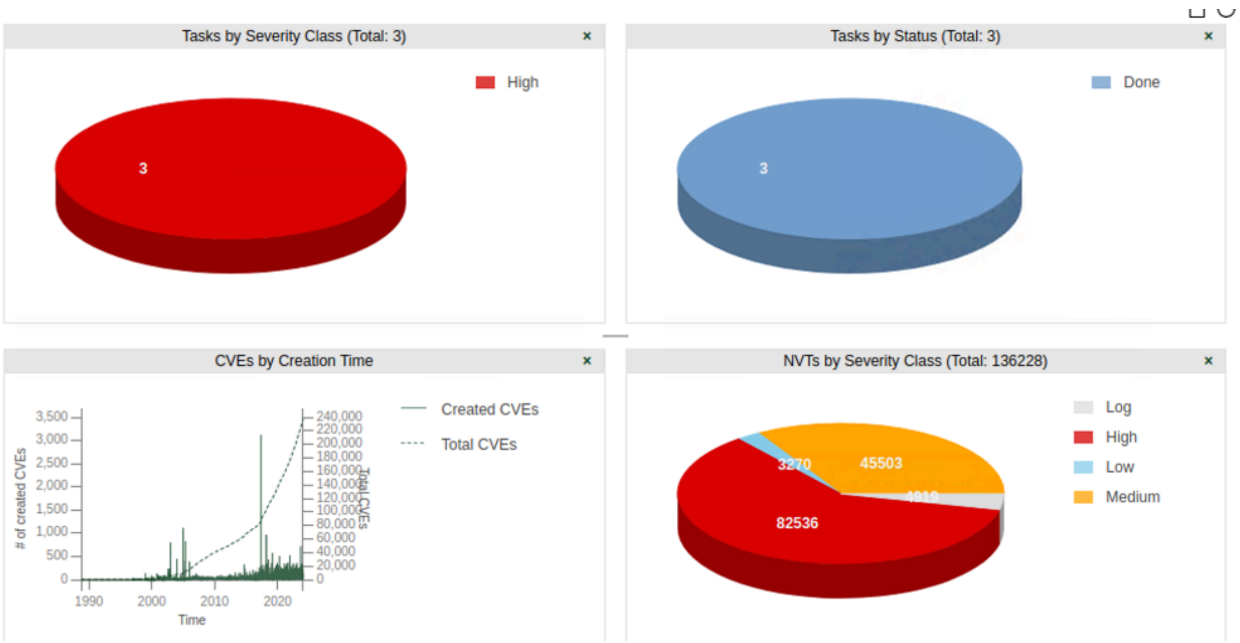
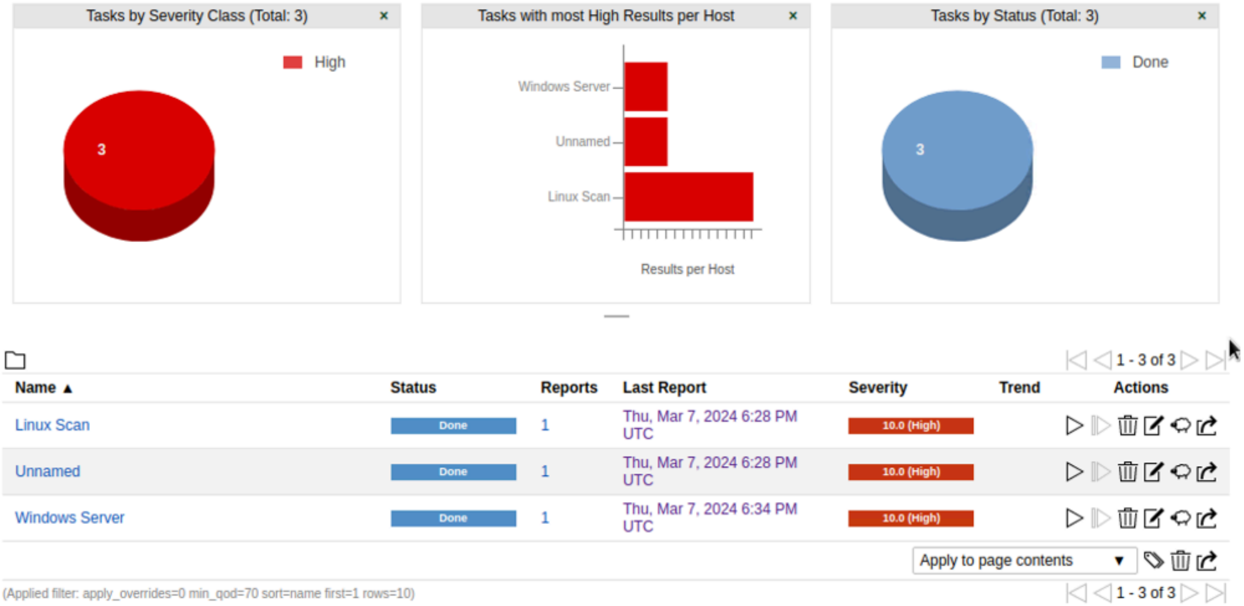


Fig.1 Greenbone Vulnerability Management Interface Overview


Tasks by Severity Class (Total: 3)
High
3
Tasks with most High Results per Host
Windows Server
Unnamed
Linux Scan
Results per Host
Tasks by Status (Total: 3)
Done
3
1 - 3 of 3

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Linux Scan	Done	1	Thu, Mar 7, 2024 6:28 PM UTC	10.0 (High)		
Unnamed	Done	1	Thu, Mar 7, 2024 6:28 PM UTC	10.0 (High)		
Windows Server	Done	1	Thu, Mar 7, 2024 6:34 PM UTC	10.0 (High)		

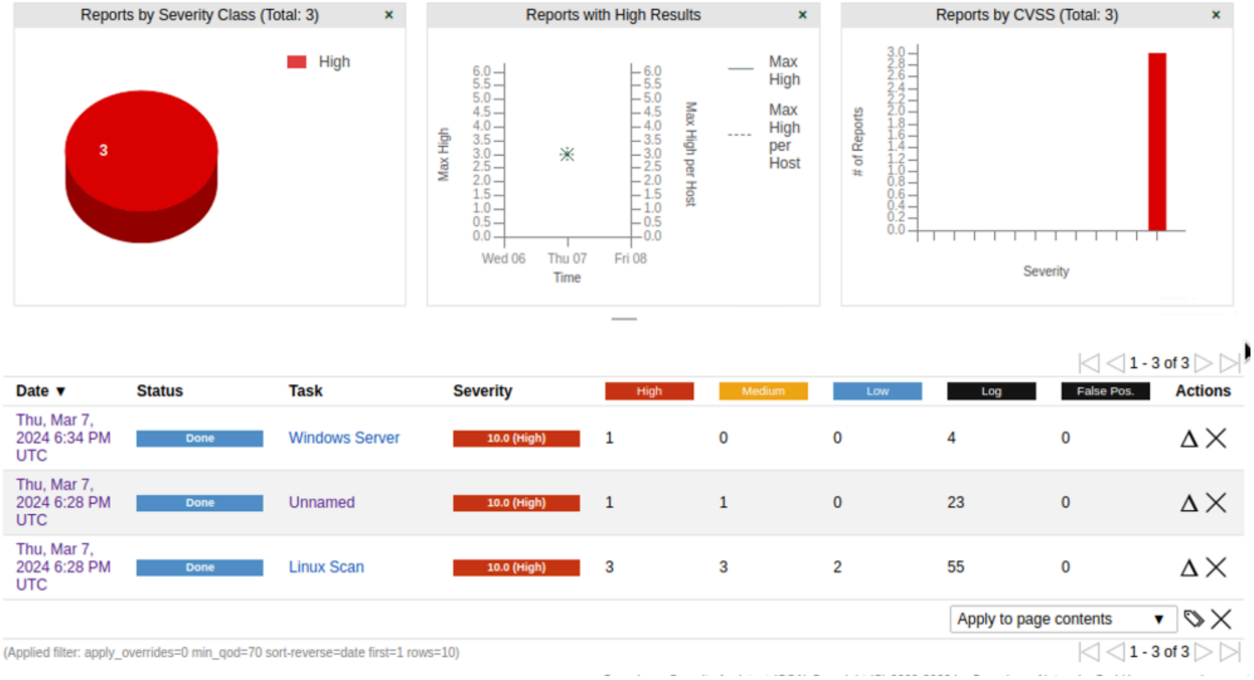
Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 3 of 3

Fig.2 Greenbone Vulnerability Management Interface Tasks

Appendix B



1 - 3 of 3

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Thu, Mar 7, 2024 6:34 PM UTC	Done	Windows Server	10.0 (High)	1	0	0	4	0	∆ ✕
Thu, Mar 7, 2024 6:28 PM UTC	Done	Unnamed	10.0 (High)	1	1	0	23	0	∆ ✕
Thu, Mar 7, 2024 6:28 PM UTC	Done	Linux Scan	10.0 (High)	3	3	2	55	0	∆ ✕

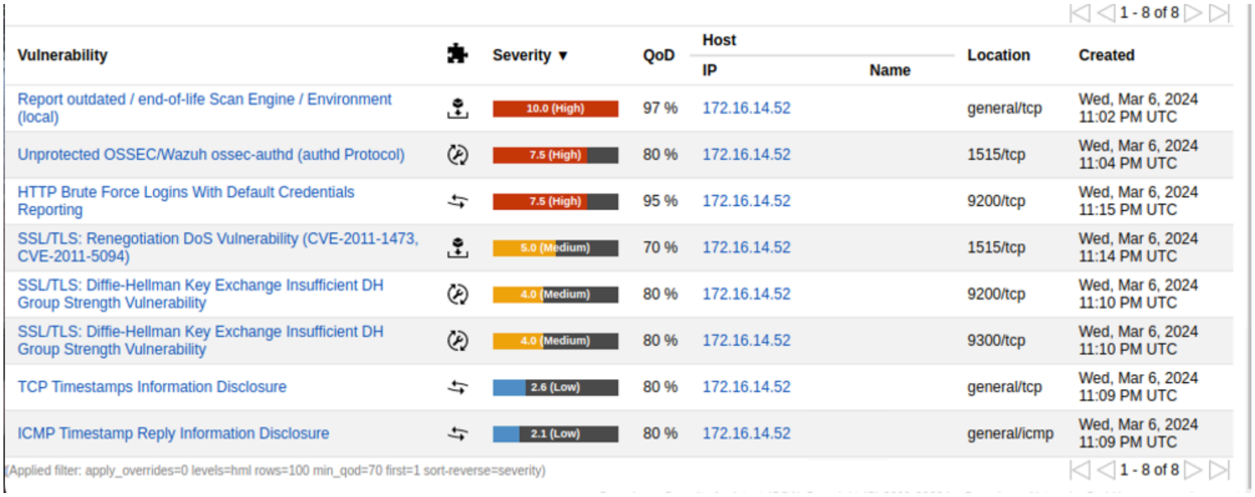
Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

1 - 3 of 3

Fig.3 Greenbone Vulnerability Management Interface Reports

Linux



1 - 8 of 8

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	172.16.14.52		general/tcp	Wed, Mar 6, 2024 11:02 PM UTC
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)		7.5 (High)	80 %	172.16.14.52		1515/tcp	Wed, Mar 6, 2024 11:04 PM UTC
HTTP Brute Force Logins With Default Credentials Reporting		7.5 (High)	95 %	172.16.14.52		9200/tcp	Wed, Mar 6, 2024 11:15 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)		5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Wed, Mar 6, 2024 11:14 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52		9200/tcp	Wed, Mar 6, 2024 11:10 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52		9300/tcp	Wed, Mar 6, 2024 11:10 PM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.52		general/tcp	Wed, Mar 6, 2024 11:09 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.52		general/icmp	Wed, Mar 6, 2024 11:09 PM UTC

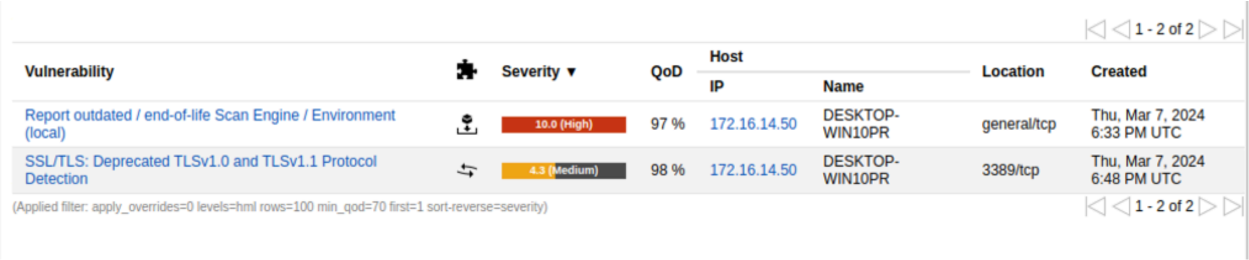
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 8 of 8

Fig. 4 Greenbone Vulnerability Management Interface, Scan Results, Linux

Appendix C

Windows1

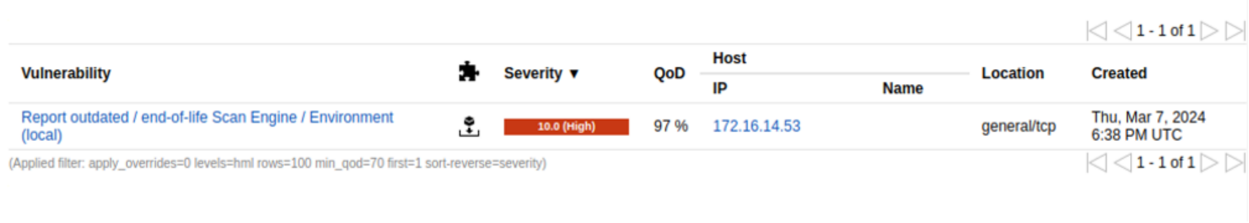


Vulnerability	Severity ▼	QoD	Host		Location	Created
			IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.50	DESKTOP-WIN10PR	general/tcp	Thu, Mar 7, 2024 6:33 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.50	DESKTOP-WIN10PR	3389/tcp	Thu, Mar 7, 2024 6:48 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Fig. 5 Greenbone Vulnerability Management Interface, Scan Results, Windows1

Winserver



Vulnerability	Severity ▼	QoD	Host		Location	Created
			IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.53		general/tcp	Thu, Mar 7, 2024 6:38 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Fig. 6 Greenbone Vulnerability Management Interface, Scan Results, Winserver