Cat’s Company Vulnerabilities

Prepared by: Anastasiya Gruneva
Date: January 20th, 2025

Table of Contents

Executive Summary

On January 17th, 2025, a vulnerability assessment was conducted to identify and address security weaknesses in two critical systems: a Linux server and a Windows 11 machine. The assessment, using OpenVAS, revealed one high-severity vulnerability and six others of medium and low severity. These vulnerabilities present risks such as unauthorized access to sensitive customer data, exposure of credentials, and potential downtime for critical services.

The high-severity FTP vulnerability poses the most significant risk, as it could lead to data breaches, compliance violations, and reputational harm. Medium-severity issues, like unencrypted HTTP connections, increase the risk of credential theft, which could disrupt operations. Fixing these vulnerabilities quickly will help protect sensitive data, ensure compliance, and reduce downtime.

The following actions are recommended in priority order:

1. Immediate remediation of high-severity risks by implementing strong password policies, disabling weak credentials, and enforcing multi-factor authentication (MFA).
2. Addressing medium-severity risks by enforcing HTTPS for secure communication, disabling anonymous FTP logins and transitioning to secure protocols like SFTP/FTPS.
3. Mitigating low-severity risks by disabling TCP/ICMP timestamp responses to reduce reconnaissance opportunities.
4. Long-term policy updates to enhance security posture, including regular vulnerability scanning, secure configuration management, and staff training.

This proactive approach ensures the protection of sensitive data and fortifies system defenses against potential threats, aligning with NIST and MITRE guidelines.

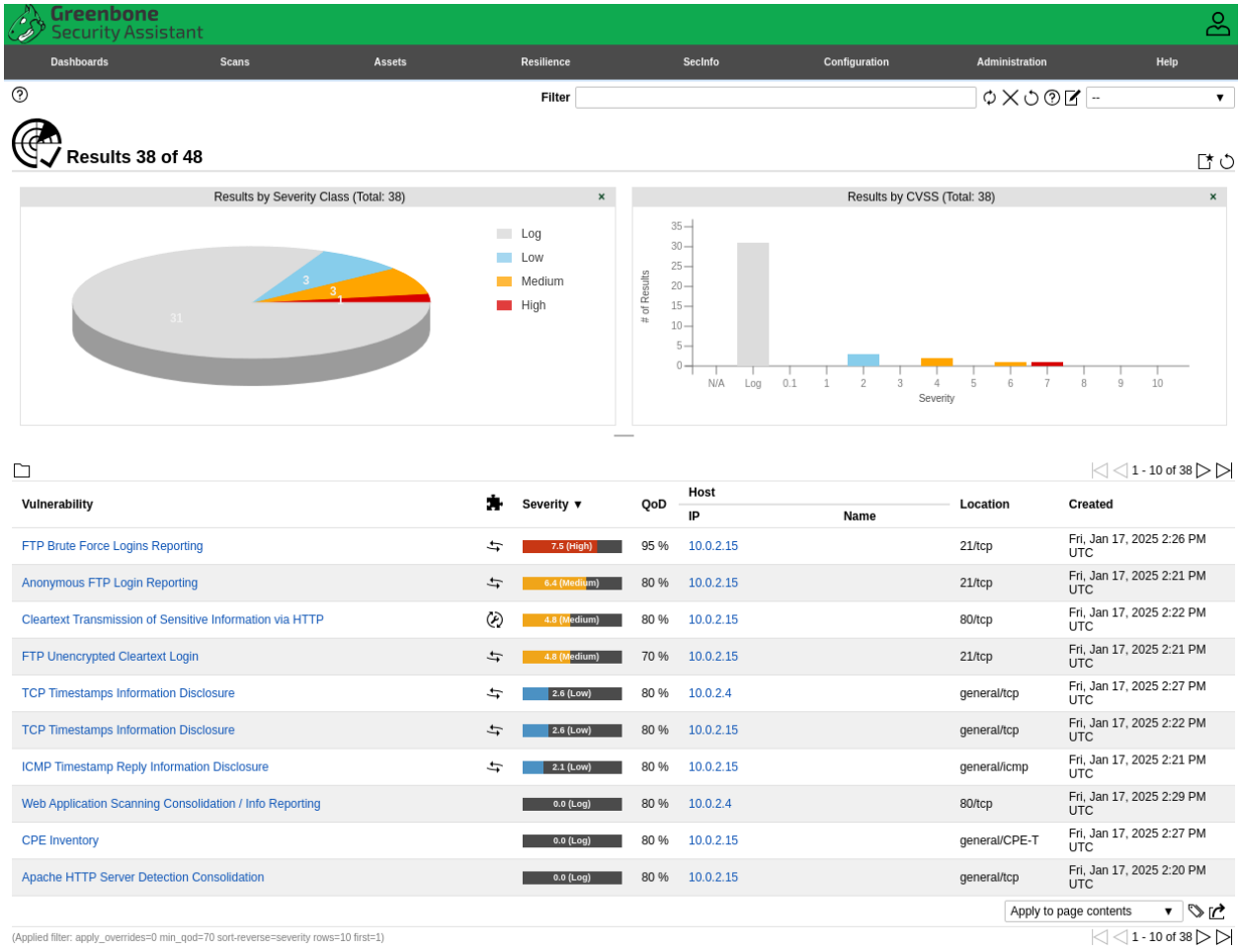
Vulnerability Assessment Report

Scan Results

This report contains the output of vulnerability assessment conducted January 17th, 2025.

Hosts scanned:

- 10.0.2.15 - Linux Server Machine
- 10.0.2.4 - Windows 11 Machine



Vulnerability	Severity	QoD	Host IP	Host Name	Location	Created
FTP Brute Force Logins Reporting	7.5 (High)	95 %	10.0.2.15		21/tcp	Fri, Jan 17, 2025 2:26 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	10.0.2.15		21/tcp	Fri, Jan 17, 2025 2:21 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	10.0.2.15		80/tcp	Fri, Jan 17, 2025 2:22 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.0.2.15		21/tcp	Fri, Jan 17, 2025 2:21 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.0.2.4		general/tcp	Fri, Jan 17, 2025 2:27 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.0.2.15		general/tcp	Fri, Jan 17, 2025 2:22 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	10.0.2.15		general/icmp	Fri, Jan 17, 2025 2:21 PM UTC
Web Application Scanning Consolidation / Info Reporting	0.0 (Log)	80 %	10.0.2.4		80/tcp	Fri, Jan 17, 2025 2:29 PM UTC
CPE Inventory	0.0 (Log)	80 %	10.0.2.15		general/CPE-T	Fri, Jan 17, 2025 2:27 PM UTC
Apache HTTP Server Detection Consolidation	0.0 (Log)	80 %	10.0.2.15		general/tcp	Fri, Jan 17, 2025 2:20 PM UTC

Figure 1. Scan results.

In short, 1 high, 3 medium, and 3 low-level findings are detected, and the details are given below.

Methodology

Tool used: OpenVAS (Open Vulnerability Assessment Scanner).

- Purpose: To perform an automated security scan and detect vulnerabilities in the target systems, including misconfigurations, unpatched software, weak credentials, and other security weaknesses. Also ensure coverage of a broad range of known vulnerabilities (CVE database).

Type of Scan Conducted: Full and Fast Vulnerability Scan.

- Purpose: Detect known vulnerabilities, misconfigurations, and weak credentials in the target systems.

This scan configuration is based on the information gathered in the previous port scan and uses almost all vulnerability tests (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. The other “Full” configurations only provide more value in rare cases but with much higher effort (Greenbone Enterprise Appliance with Greenbone OS 22.04 – Manual, 2025).

Environments Scanned:

- Linux Server Machine: A virtual machine running Ubuntu. The server hosted services such as FTP, HTTP, MySQL and Apache, which were actively tested during the scan.
- Windows Machine: A virtual machine running Windows 11. The machine hosted HTTP service.

Findings

All two hosts were successfully scanned and 1 high, 3 medium, and 3 low-level findings were detected. Details by Severity:

High Severity (CVSS 7.5)

1. It was possible to login into the remote FTP server using weak/known credentials. **Service:** FTP (Port 21/tcp). **Impact:** This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Medium Severity (CVSS 4.8-6.4)

1. The host/application transmits sensitive information (username, passwords) in cleartext via HTTP. **Service:** HTTP (Port 80/tcp). **Impact:** Anattacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
2. Reports if the remote FTP Server allows anonymous logins. **Service:** FTP (Port 21/tcp). **Impact:** Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
   - gain access to sensitive files
   - upload or delete files.
3. The remote host is running a FTP service that allows cleartext logins over unencrypted connections. **Service:** FTP (Port 21/tcp). **Impact:** An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Low Severity (CVSS 2.1-2.6)

1. The remote host implements TCP timestamps and therefore allows to compute the uptime. **Service:** general/tcp. **Impact:** A side effect of this feature is that the uptime of the remote host can sometimes be computed. This vulnerability was detected on both machines.
2. The remote host responded to an ICMP timestamp request. **Service:** general/icmp. **Impact:** This information could theoretically be used to exploit weak time-based random number generators in other services.

See details in raw scan report in Appendix A and Appendix B.

Risk Assessment

To classify and prioritize vulnerabilities, the following risk categories are used (OWASP Risk Rating Methodology, 2025):

Critical Severity

- Definition: Vulnerabilities that pose an imminent risk of system compromise or unauthorized access. Exploitation could lead to severe impacts like data breaches, complete system compromise, or denial of service.
- CVSS Score Range: 9.0 - 10.0.
- Examples: Unpatched critical software vulnerabilities, active exploitation in the wild.

High Severity

- Definition: Vulnerabilities that could allow an attacker to gain unauthorized access or compromise the confidentiality, integrity, or availability of the system. Requires immediate remediation.
- CVSS Score Range: 7.0 - 8.9.
- Examples: Weak credentials allowing unauthorized access.

Medium Severity

- Definition: Vulnerabilities that pose a moderate threat and could lead to a potential breach or misuse if exploited. Mitigation should occur promptly but not urgently.
- CVSS Score Range: 4.0 - 6.9
- Examples: Sensitive data transmitted over unencrypted channels.

Low Severity

- Definition: Vulnerabilities with minimal impact or likelihood of exploitation. These issues generally require long-term mitigation but do not pose an immediate threat.
- CVSS Score Range: 0.1 - 3.9
- Examples: Non-critical information leakage like uptime visibility.

Table 1. Detailed Vulnerability Descriptions and Mitigation Recommendations

Vulnerability	Severity Level	Description	Solution	Count
Weak/ known credentials for FTP server login	High (CVSS 7.5)	The FTP server on the Linux machine allows login using weak or default credentials, exposing the system to unauthorized access.	Implement strong password policies. Disable weak/default credentials. Enforce multi-factor authentication (MFA) where possible. References: NIST SP 800-63B, MITRE CWE-521.	1
Anonymous FTP logins permitted CVE-1999-0497	Medium (CVSS 6.4)	The Linux server's FTP service permits anonymous logins, potentially granting unauthorized access to files.	Disable anonymous FTP logins. Use secure alternatives like SFTP or FTPS. References: NIST SP 800-123, MITRE CWE-276.	1

Sensitive information transmitted in cleartext via HTTP	Medium (CVSS 4.8)	HTTP service Linux server transmits sensitive data, making it susceptible to interception.	Enforce the use of HTTPS by deploying SSL/TLS certificates. Redirect HTTP traffic to HTTPS. References: NIST SP 800-52, MITRE CWE-319.	1
FTP service allows cleartext logins	Medium (CVSS 4.8)	FTP traffic on the Linux server is unencrypted, exposing credentials to network sniffing attacks.	Replace FTP with secure protocols like SFTP or FTPS. Encrypt all communications. References: NIST SP 800-45, MITRE CWE-522.	1
TCP timestamps enable uptime calculation	Low (CVSS 2.6)	TCP timestamp responses allow attackers to deduce system uptime, which could aid in reconnaissance.	Disable TCP timestamp responses via system configurations. References: MITRE CWE-200.	2
ICMP timestamp response leaks information CVE-1999-0524	Low (CVSS 2.1)	ICMP timestamp responses reveal time-based information that could potentially be used to exploit weak random number generators.	Block or restrict ICMP timestamp requests via firewall rules. References: NIST SP 800-41, MITRE CWE-200.	1

Recommendations

Immediate - High-Severity Vulnerabilities

1. Actions: Implement strong password policies. Disable weak/default credentials. Enforce multi-factor authentication (MFA) where possible.

References: NIST SP 800-63B, MITRE CWE-521.

Explanation: Weak credentials pose the most immediate risk by enabling unauthorized access to sensitive systems.

Medium - Medium-Severity Vulnerabilities

1. Actions: Disable anonymous FTP logins. Use secure alternatives like SFTP or FTPS.

References: NIST SP 800-123, MITRE CWE-276.
Explanation: Anonymous access can lead to unauthorized data modification or exposure.

2. Actions: Enforce the use of HTTPS by deploying SSL/TLS certificates. Redirect HTTP traffic to HTTPS.

References: NIST SP 800-52, MITRE CWE-319.
Explanation: Unencrypted data transmission exposes sensitive information to interception, which could lead to credential theft or data leaks.

3. Actions: Replace FTP with secure protocols like SFTP or FTPS. Encrypt all communications.

References: NIST SP 800-45, MITRE CWE-522.
Explanation: Cleartext logins are vulnerable to sniffing attacks, compromising user credentials.

Long term - Low-Severity Vulnerabilities

1. Actions: Disable TCP timestamp responses via system configurations.

References: MITRE CWE-200.
Explanation: Though not critical, this reduces reconnaissance capabilities for potential attackers.

2. Actions: Block or restrict ICMP timestamp requests via firewall rules.

References: NIST SP 800-41, MITRE CWE-200.
Explanation: Prevents the disclosure of system timing data, which could indirectly aid attacks.

Security Policy Recommendations

1. Implement a Strong Password Policy
    - Require complex passwords (minimum length, special characters, etc.).
    - Regularly rotate passwords and enforce expiration policies.
    - Use multi-factor authentication (MFA) wherever possible.
2. Mandate Secure Protocols
    - Enforce HTTPS for all web services.
    - Transition from FTP to SFTP/FTPS for file transfers.
    - Ensure all communication channels are encrypted.
3. Regular Vulnerability Scanning and Patch Management

- Conduct regular scans using tools like OpenVAS to detect new vulnerabilities.
- Implement a patch management process to ensure timely updates to software and firmware.

4. Firewall and Network Configuration
    - Restrict unnecessary ports and services.
    - Block or limit ICMP responses unless explicitly required.
    - Enable logging and monitoring of network traffic for anomalies.
5. Training and Awareness
    - Train employees on the importance of secure credentials and recognizing phishing attempts.
    - Conduct periodic security awareness sessions to maintain a proactive security culture.

References

Greenbone Enterprise Appliance with Greenbone OS 22.04 – Manual. (retrieved 20-01-2025)
https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html#scanconfigs

OWASP Risk Rating Methodology. (retrieved 20-01-2025)
https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

National Institute of Standards and Technology (NIST) Special Publications. (retrieved 20-01-2025) https://csrc.nist.gov/publications

MITRE Common Weakness Enumeration (CWE) Database. (retrieved 20-01-2025)
https://cwe.mitre.org/

RSI Security. Tips For Creating a Strong Vulnerability Assessment Report. (26-09-2019)
https://blog.rsisecurity.com/tips-for-creating-a-strong-vulnerability-assessment-report/

S4E.io. 5 Steps of Vulnerability Assessment Report and How to Write an Assessment Report? (02-03-2021)
https://resources.s4e.io/blog/a-good-vulnerability-assessment-and-how-to-write-report/

Sahoo, P. (17-01-2025). Vulnerability Assessment Report: A Complete Guide.
https://qualysec.com/vulnerability-assessment-reports-a-complete-guide/

Appendix A. Raw Scan Report (host 10.0.2.15)

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 6 results selected by the
filtering described above. Before filtering there were 33 results.

Scan started: Fri Jan 17 14:19:21 2025 UTC
Scan ended: Fri Jan 17 14:27:09 2025 UTC
Task: W5D4 scan LinuxVM

Host Summary
****

Host	High	Medium	Low	Log	False Positive
10.0.2.15	1	3	2	0	0
Total: 1	1	3	2	0	0

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

Host 10.0.2.15
****

Scanning of this host started at: Fri Jan 17 14:19:48 2025 UTC
Number of results: 6

Port Summary for Host 10.0.2.15

Service (Port)	Threat Level
21/tcp	High (CVSS: 7.5)
80/tcp	Medium (CVSS: 4.8)
general/tcp	Low (CVSS: 2.6)
general/icmp	Low (CVSS: 2.1)

Security Issues for Host 10.0.2.15

Issue

NVT: FTP Brute Force Logins Reporting
OID: 1.3.6.1.4.1.25623.1.0.108718
Threat: High (CVSS: 7.5)
Port: 21/tcp

Summary:
It was possible to login into the remote FTP server using
weak/known credentials.

Vulnerability Detection Result:
It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
user:user

Impact:

This issue may be exploited by a remote attacker to e.g. gain
  access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight:
The following devices are / software is known to be affected:
  - CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA!
 P&R
  - CVE-2013-7404: GE Healthcare Discovery NM 750b
  - CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
  - CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
  - CVE-2016-8731: Foscam C1 devices
  - CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
  - CVE-2018-9068: IMM2 for IBM and Lenovo System x
  - CVE-2018-17771: Ingenico Telium 2 PoS terminals
  - CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
  Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) m!
ight run into a
  timeout the actual reporting of this vulnerability takes place in this VT inst!
ead.

Vulnerability Detection Method:
Reports weak/known credentials detected by the VT
  'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details:
FTP Brute Force Logins Reporting
(OID: 1.3.6.1.4.1.25623.1.0.108718)
Version used: 2024-08-30T05:05:38Z

References:
 cve: CVE-1999-0501
 cve: CVE-1999-0502
 cve: CVE-1999-0507
 cve: CVE-1999-0508
 cve: CVE-2001-1594
 cve: CVE-2013-7404
 cve: CVE-2014-9198

cve: CVE-2015-7261
cve: CVE-2016-8731
cve: CVE-2017-8218
cve: CVE-2018-9068
cve: CVE-2018-17771
cve: CVE-2018-19063
cve: CVE-2018-19064

Issue

NVT: Anonymous FTP Login Reporting
OID: 1.3.6.1.4.1.25623.1.0.900600
Threat: Medium (CVSS: 6.4)
Port: 21/tcp

Summary:
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result:
It was possible to login to the remote FTP service with the following anonymous !
account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
drwxr-xr-x 2 ftp ftp 4096 Sep 28 22:49 pub
Account "ftp":
drwxr-xr-x 2 ftp ftp 4096 Sep 28 22:49 pub

Impact:
Based on the files accessible via this anonymous FTP login and
the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous
logins.

Vulnerability Insight:
A host that provides an FTP service may additionally provide
  Anonymous FTP access as well. Under this arrangement, users do not strictly ne!
ed an account on the
  host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for!
 username. Although
  users are commonly asked to send their email address as their password, little!
 to no verification
  is actually performed on the supplied data.
  Remark: NIST don't see 'configuration issues' as software flaws so the referen!
ced CVE has a
  severity of 0.0. The severity of this VT has been raised by Greenbone to still!
 report a
  configuration issue on the target.

Vulnerability Detection Method:
Details:
Anonymous FTP Login Reporting
(OID: 1.3.6.1.4.1.25623.1.0.900600)
Version used: 2021-10-20T09:03:29Z

References:
 cve: CVE-1999-0497

Issue

NVT: FTP Unencrypted Cleartext Login
OID: 1.3.6.1.4.1.25623.1.0.108528
Threat: Medium (CVSS: 4.8)
Port: 21/tcp

Summary:
The remote host is running a FTP service that allows cleartext logins over
  unencrypted connections.

Vulnerability Detection Result:
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command!
. Response(s):

Non-anonymous sessions: 331 Please specify the password.

Impact:
An attacker can uncover login names and passwords by sniffing traffic to the
FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see
the manual of the FTP service for more information.

Vulnerability Detection Method:
Tries to login to a non FTPS enabled FTP service without sending a
'AUTH TLS' command first and checks if the service is accepting the login with!
out enforcing the use of
the 'AUTH TLS' command.
Details:
FTP Unencrypted Cleartext Login
(OID: 1.3.6.1.4.1.25623.1.0.108528)
Version used: 2023-12-20T05:05:58Z

Issue

NVT: Cleartext Transmission of Sensitive Information via HTTP
OID: 1.3.6.1.4.1.25623.1.0.108440
Threat: Medium (CVSS: 4.8)
Port: 80/tcp

Summary:
The host / application transmits sensitive information (username, passwords) in
cleartext via HTTP.

Vulnerability Detection Result:
The following input fields were identified (URL:input name):
http://10.0.2.15/:httpd_password

Impact:
An attacker could use this situation to compromise or eavesdrop on the
HTTP communication between the client and the server using a man-in-the-middle!

attack to get access to
sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
Additionally make sure the host / application is redirecting all users to the !
secured SSL/TLS connection before
allowing to input sensitive data into the mentioned functions.

Affected Software/OS:
Hosts / applications which doesn't enforce the transmission of sensitive data vi!
a an
encrypted SSL/TLS connection.

Vulnerability Detection Method:
Evaluate previous collected information and check if the host / application is n!
ot
enforcing the transmission of sensitive data via an encrypted SSL/TLS connecti!
on.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details:
Cleartext Transmission of Sensitive Information via HTTP
(OID: 1.3.6.1.4.1.25623.1.0.108440)
Version used: 2023-09-07T05:05:21Z

References:
url:
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Sessio
n_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

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: 2987732173
Packet 2: 2987733248

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.aspx?id=9152
 url: https://www.fortiguard.com/psirt/FG-IR-16-090

Issue

NVT: ICMP Timestamp Reply Information Disclosure
OID: 1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port: general/icmp

Summary:
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically be used to exploit weak
  time-based random number generators in other services.

Solution:

Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing throug!
h the firewall in
either direction (either completely or only for untrusted networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP message which replies to a
Timestamp message. It consists of the originating timestamp sent by the sender!
of the Timestamp as
well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13) request and checks if a
Timestamp Reply (Type 14) is received.
Details:
ICMP Timestamp Reply Information Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2023-05-11T09:09:33Z

References:
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

Appendix B. Raw Scan Report (host 10.0.2.4)

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 result 1 of the 1 results selected by the
filtering above. Before filtering there were 15 results.

Scan started: Fri Jan 17 14:19:31 2025 UTC
Scan ended: Fri Jan 17 14:32:49 2025 UTC
Task: W5D4 scan WindowsVM

Host Summary
****

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

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

Host 10.0.2.4
****

Scanning of this host started at: Fri Jan 17 14:19:57 2025 UTC
Number of results: 1

Port Summary for Host 10.0.2.4

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

Security Issues for Host 10.0.2.4

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: 649551
Packet 2: 650606

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.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090