NessusReportsPro

VULNERABILITY ASSESSMENT REPORT

Your Logo Here

Prepared for Client X

Scan date: March 3, 2026
Report generated date: March 26, 2026

Your Logo Here

Contents

Your Logo Here

Introduction/Summary

This report summarizes the results of a Nessus vulnerability scan performed on assets within the client-defined scope. The analysis and findings presented in this document are derived exclusively from Nessus scan result data provided by the client in the form of exported scan files. No vulnerability scanning activities were conducted by the report author as part of this engagement.

Nessus scan results are designed to identify known software vulnerabilities, missing security patches, and potential configuration weaknesses that may impact the security posture of the assessed systems. The results contained in the provided data may originate from credentialed or non-credentialed scans depending on how the scans were originally configured and executed by the client.

The purpose of this report is to organize and present the vulnerabilities identified within the provided scan data, describe the associated risks, and provide information to assist stakeholders in understanding and prioritizing remediation activities.

Report Scope and Methodology

1. Nessus vulnerability scan results provided by the client were reviewed and analyzed for the assets listed within the defined scope. No vulnerability scanning activities were conducted as part of this engagement; the analysis is based solely on scan results supplied by the client.
2. Automated processing tools were used to parse and organize the provided Nessus scan data, grouping related vulnerabilities to produce a structured and readable report format.
3. This report summarizes the vulnerabilities identified in the scan results and provides context to assist stakeholders in evaluating potential risks and remediation priorities.
4. The systems included in the scope of the assessment are listed below:
    - 111.111.111.111 – 111.111.111.180

Your Logo Here

Vulnerability Severity Levels

The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity.

SEVERITY LEVEL	CVSS SCORE	DEFINITION
Critical	9.0 - 10.0	Attackers may be able to access sensitive data and run code on your application or supporting infrastructure.
High	7.0 - 8.9	Attackers may be able to access sensitive data on your application.
Medium	4.0 - 6.9	Attackers may be able to access sensitive data on your application under some conditions.
Low	0.0 - 3.9	The application may provide information that could be used to exploit other vulnerabilities and attack the application.

Finding Summary

The chart below presents two key metrics used to summarize the scan results. **Unique** findings represent distinct vulnerability types identified, while **Total** vulnerabilities represent the total number of affected instances across all in-scope assets, calculated by multiplying the number of unique findings by the number of impacted hosts.

SEVERITY	CVSS	TOTAL	UNIQUE
CRITICAL	9.0 - 10.0	0	0
HIGH	7.0 - 8.9	4	1
MEDIUM	4.0 - 6.9	8	2
LOW	0.0 - 3.9	20	1

Your Logo Here

Executive Summary

The hosts have vulnerabilities due to several configuration weaknesses, including:

1. High Risk: Support for medium-strength SSL/TLS ciphers (SWEET32) increases exposure to cryptographic attacks.
   Recommendation: Disable medium-strength ciphers and enforce strong encryption standards.
2. Medium Risk: Legacy TLS protocols configuration-related weaknesses are enabled.
   Recommendation: Disable TLS 1.0/1.1 and enforce TLS 1.2 or higher (preferably TLS 1.3).
3. Low Risk: ICMP timestamp responses expose system time information.
   Recommendation: Block ICMP timestamp requests (type 13) and replies (type 14).

Vulnerabilities

HIGH - SSL MEDIUM STRENGTH CIPHER SUITES SUPPORTED (SWEET32)

CVEs	CVE-2016-2183
CVSS_V3	High – 7.5
CVSS_V2	Medium – 5.0
VPR	Medium – 6.1
Exploitability Ease	No known public exploits
Host(s)	111.111.111.111, 111.111.111.112, 111.111.111.113, 111.111.111.114

SYNOPSIS

The remote service supports the use of medium strength SSL ciphers.

DESCRIPTION

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

SEE ALSO

- http://www.nessus.org/u?df5555f5
- https://sweet32.info

SOLUTION

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

OUTPUT

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth
Encryption             MAC
    ----------------------        ----------       ---           ----     -
--------------------  ---
```

```
    DES-CBC3-SHA                0x00, 0x0A       RSA           RSA
3DES-CBC(168)          SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

MEDIUM - TLS VERSION 1.0 PROTOCOL DETECTION

CVEs	N/A
CVSS_V3	Medium – 6.5
CVSS_V2	Medium – 6.1
VPR	N/A
Exploitability Ease	No known public exploits
Host(s)	111.111.111.111, 111.111.111.112, 111.111.111.113, 111.111.111.114

SYNOPSIS

The remote service encrypts traffic using an older version of TLS.

DESCRIPTION

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

SEE ALSO

- https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

SOLUTION

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

OUTPUT

```
TLSv1 is enabled and the server supports at least one cipher.
```

MEDIUM - TLS VERSION 1.1 DEPRECATED PROTOCOL

CVEs	N/A
CVSS_V3	Medium – 6.5
CVSS_V2	Medium – 6.1
VPR	N/A
Exploitability Ease	No known public exploits
Host(s)	111.111.111.111, 111.111.111.112, 111.111.111.113, 111.111.111.114

SYNOPSIS

The remote service encrypts traffic using an older version of TLS.

DESCRIPTION

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

SEE ALSO

- http://www.nessus.org/u?c8ae820d
- https://datatracker.ietf.org/doc/html/rfc8996

SOLUTION

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

OUTPUT

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

LOW - ICMP TIMESTAMP REQUEST REMOTE DATE DISCLOSURE

CVEs	CVE-1999-0524
CVSS_V3	N/A
CVSS_V2	Low – 2.1
VPR	Low – 2.2
Exploitability Ease	No known public exploits
Host(s)	111.111.111.111, 111.111.111.112, 111.111.111.113, 111.111.111.114, 111.111.111.115, 111.111.111.116, 111.111.111.117, 111.111.111.118, 111.111.111.119, 111.111.111.120, 111.111.111.121, 111.111.111.122, 111.111.111.123, 111.111.111.124, 111.111.111.125, 111.111.111.126, 111.111.111.127, 111.111.111.128, 111.111.111.129, 111.111.111.130

SYNOPSIS

It is possible to determine the exact time set on the remote host.

DESCRIPTION

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

SEE ALSO

N/A

SOLUTION

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

OUTPUT

```
The difference between the local and remote clocks is 1 second.
```