

Client Final Report Infrastructure Vulnerability Project

V 1.0

September 12, 2024

Designed to deliver the final project outcome information about an organization's network and systems infrastructure vulnerabilities.



Table of Contents

1.0 XXX Vulnerability Report

1.1 Introduction

1.2 Objective

2.0 High-Level Summary

2.1 Recommendations

3.0 Methodologies

3.1 Information Gathering

3.2 Vulnerability Assessment

System IP: 192.168. ()

Service Enumeration

Vulnerability #1

Vulnerability #2

System IP: 192.168. ()

Service Enumeration

Vulnerability #1

Vulnerability #2

System IP: 192.168. ()

Service Enumeration

Vulnerability #1

Vulnerability #2

Appendix: Informational Vulnerability Assessments



1.0 Vulnerability Report

1.1 Introduction

This Vulnerability Report provides a comprehensive analysis of potential security weaknesses identified within the specified system, application, or network. Its primary goal is to help stakeholders understand the risks these vulnerabilities pose and recommend steps to mitigate or eliminate them.

The report is based on a thorough assessment conducted through various methods, including automated scans, manual testing, and code reviews. It highlights both critical and low-priority vulnerabilities to provide a holistic view of the security posture.

In the following sections, you will find a detailed description of each identified vulnerability, its potential impact, and recommended remediation strategies. By addressing these vulnerabilities, can improve its overall security and reduce the risk of cyberattacks.

1.2 Objective

The primary objective of this Vulnerability Report is to identify and assess security vulnerabilities within the targeted system, application, or network. This assessment aims to:

- Uncover Potential Security Weaknesses Identify vulnerabilities that may be exploited by malicious actors, including both internal and external threats.
- Evaluate Risk Levels Determine the potential impact and likelihood of each identified vulnerability being exploited.
- Recommend Remediation Strategies Provide actionable recommendations to mitigate or eliminate vulnerabilities, thereby reducing overall security risks.
- Improve Security Posture Assist the organization in strengthening its defenses against future attacks by identifying areas for improvement.
- Compliance and Standards Ensure that the organization adheres to relevant security frameworks, regulations, and industry best practices.



The assessment is designed to provide a clear path toward enhancing the security of the system while minimizing disruptions to operations.

2.0 High-Level Summary

I conducted an external virtual box vulnerability assessment against the client's digital infrastructure. An external virtual box vulnerability assessment is a rigorous evaluation of the systems that are exposed to the internet without any internal network access or prior knowledge. Tools used were OpenVAS, NMAP, and Nessus. The primary aim of this assessment was to simulate an adversary's approach to compromise the client's externally accessible systems and to infiltrate the organization's external defense mechanisms. Our fundamental goal was to meticulously scrutinize the network, catalog externally accessible systems, exploit any vulnerabilities present, and document our findings to the client.



The implicated systems, along with a succinct synopsis of the exploitation methods, are itemized as follows:

IP	Summary	Risk Rating	Comments
41.	Apache HTTP Server (DOS)	High	Denial of Service (DoS) Attacks: This refers to the vulnerability of the Apache HTTP Server to Denial-of-Service attacks.
41.	SSL Certificate Cannot Be Trusted	Medium	Generally, means that your browser or server cannot verify the authenticity of the certificate.
41.	SSL Self-Guided Certificate	Medium	This type of certificate provides encryption but doesn't offer the validation and trust that certificates issued by recognized CAs provide.
102.	Missing Cookie Attribute (HTTP)	Medium	When an HTTP cookie is missing attributes, it may pose security risks or affect functionality.
102.	Missing 'HTTPOnly' Cookie Attribute	Medium	Indicates that the cookie is accessible via client-side JavaScript, which can expose it to cross-site scripting (XSS) attacks.
102.	SSL/TLS: Renegotiation DOS Vulnerability	Medium	This vulnerability can potentially lead to Denial of Service (DoS) attacks, where an attacker can overwhelm a server with renegotiation requests, leading to resource exhaustion or service degradation.
102.	Weak MAC Algorithm (s) Supported (SSH)	Low	The "Weak MAC Algorithm(s) Supported" warning in SSH indicates that the SSH server supports one or more message authentication code (MAC) algorithms that are considered weak or deprecated.



2.1 Recommendations

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3.0 Methodologies

We utilized a widely adopted approach to performing the vulnerability assessment that is effective in testing how well the clients' environments are secured.

3.1 Information Gathering

The information-gathering portion of a vulnerability assessment focuses on identifying the scope of the vulnerability assessment. The specific IP addresses were:

Client IP Addresses

- 102.
- 41.
- 102.



3.2 Vulnerability Assessment

Service Enumeration: The service enumeration portion of a vulnerability assessment focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Note:

- All identified vulnerabilities (including those classified as Low) will be included in this section.
- Informational scan results will be included in the appendix at the end of this document.





System IP: 102.

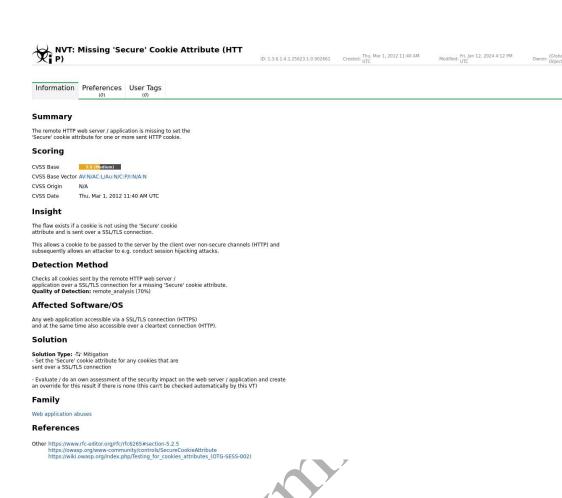
Service Enumeration

Server IP Address	Ports Open	Observations
102.	TCP: 53/80	. ~ ~
	UDP:	

Vulnerability #1

- Description: Missing Cookie Attribute (HTTP)
- CVE: N/A
- Risk Rating: 5.0
- Likelihood: Medium
- Consequence: Man-in-the-middle attacks, session hijacking, compromised confidentiality, increased risk in shared or public networks, cross-site scripting (XSS) Exploitation, and failing security best practices.
- Impact: Loss of confidentiality, Phishing and Social Engineering, and Downgrade Attacks.
- Recommendation: Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection

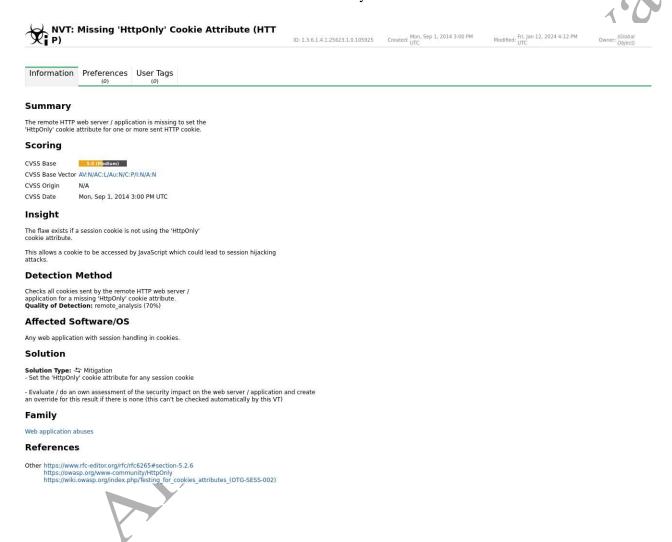




- Description: Missing 'HTTPOnly' Cookie Attribute
- CVE: N/A
- Risk Rating: 5.0



- Likelihood: Medium
- Consequence: Man-in-the-middle attacks, session hijacking, compromised confidentiality, increased risk in shared or public networks, cross-site scripting (XSS) Exploitation, and failing security best practices.
- Impact: Loss of confidentiality, Phishing and Social Engineering, and Downgrade Attacks.
- Recommendation: Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLD connection.





• Description: SSL/TLS: Renegotiation DOS Vulnerability

• CVE: 2011-1473; 2011-5094

Risk Rating: 5.0Likelihood: Medium

• Consequence: Denial of Service (DoS) Attacks, Resource Exhaustion, and Service Disruption

• Impact: Service unavailability, financial loss, reputation damage, operational lost, and compliance and legal risks.

• Recommendation: Remove/disable renegotiations capabilities altogether from/in the affected SSL/TLS service.







Information Preferences User Tags

Summary

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.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Family

SSL and TLS

References





• Description: Weak MAC Algorithm (s) Supported (SSH)

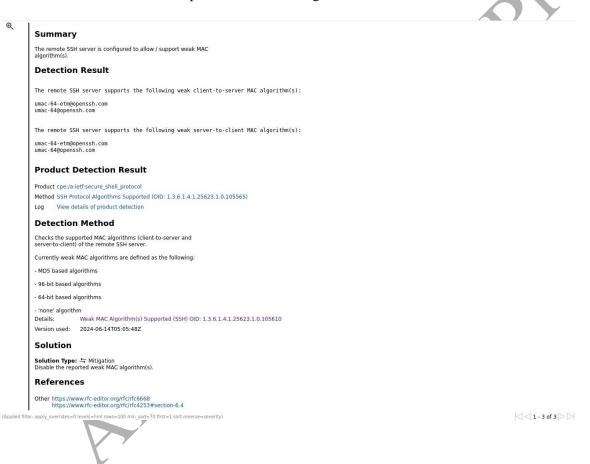
• CVE: N/A

Risk Rating: 2.6Likelihood: Low

• Consequence: Data Integrity Compromise, Authentication Bypass, Replay Attacks, Man-In-The-Middle Attacks, Cryptographic Attacks.

• Impact: Financial Loss, Reputation Damage, Impact on Encrypted Communications, and Non-Compliance with Security Standards

• Recommendation: Disable the reported weak MAC algorithm





System IP: 41.

Service Enumeration

Server IP Address	Ports Open	Observations
41.	TCP: 22/53/80	
	UDP:	

Vulnerability #1

• Description: Apache HTTP Server (DOS)

• CVE: 2011-3192/2007-6750

Risk Rating:7.8Likelihood: High

• Consequence: Disruption in service availability, often leading to denial of service for legitimate users, potentially affecting critical business operations and leading to loss of revenue or user trust.

• Impact: Disruption of services and server unavailability, with broader business and operational consequences due to downtime and performance degradation.

• Recommendation:

1. Update Apache to a patched version.

2. Disable range header processing as a temporary workaround.

3. Use WAF to block malicious requests.

4. Implement rate limiting and monitor server traffic.

5. **Deploy load balancing** to distribute traffic and reduce the risk of server overload.



```
-$ nmap -script vuln 41.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 17:50 PDT
Nmap scan report for 41.
Host is up (0.20s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
 | http-stored-xss: Couldn't find any stored XSS vulnerabilities. | http-dombased-xss: Couldn't find any DOM based XSS.
 http-vuln-cve2011-3192:
VULNERABLE:
    Apache byterange filter DoS
State: VULNERABLE
       IDs: BID:49303 CVE:CVE-2011-3192
          The Apache web server is vulnerable to a denial of service attack when numerous
          overlapping byte ranges are requested.
       Disclosure date: 2011-08-19
          https://www.tenable.com/plugins/nessus/55976
          https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
          https://www.securityfocus.com/bid/49303
          https://seclists.org/fulldisclosure/2011/Aug/175
 _http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open https
 _http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
  http-vuln-cve2010-0738:
    /jmx-console/: Authentication was not required
  http-slowloris-check:
     VULNERABLE:
     Slowloris DOS attack
       State: LIKELY VULNERABLE
       IDs: CVE:CVE-2007-6750
          Slowloris tries to keep many connections to the target web server open and hold
          them open as long as possible. It accomplishes this by opening connections to
          the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.
       Disclosure date: 2009-09-17
       References:
 Refetences:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 |
| http://ha.ckers.org/slowloris/ |
| http-crif: Couldn't find any CSRF vulnerabilities. |
| http-dombased-xs: Couldn't find any DOM based XSS.
  __http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
  http-enum:
     /blog/: Blog
     /weblog/: Blog
/weblogs/: Blog
/wordpress/: Blog
     /wiki/: Wiki
     /mediawiki/: Wiki
     /wiki/Main_Page: Wiki
     /tikiwiki/: Tikiwiki
    /cgi-bin/mj_wwwusr: Majordomo2 Mailing List
/majordomo/mj_wwwusr: Majordomo2 Mailing List
/j2ee/examples/servlets/: Oracle j2ee examples
/j2ee/examples/spy/: Oracle j2ee examples
     /dsc/: Trend Micro Data Loss Prevention Virtual Appliance
      /adr.htm: Snom IP Phone
```

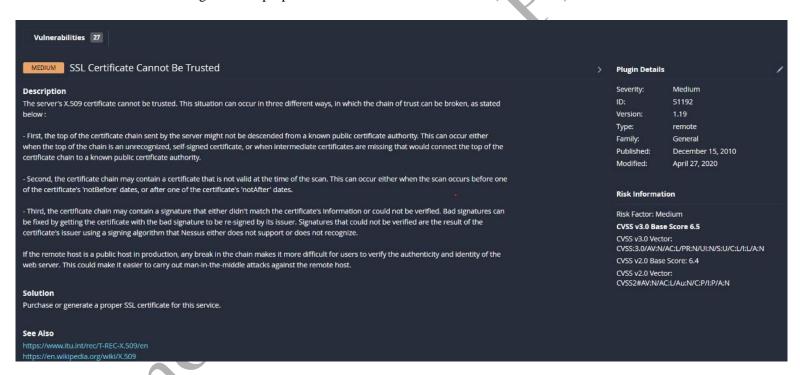


Description: SSL Certificate Cannot Be Trusted

CVE: N/A

Risk Rating: 6.5Likelihood: Medium

- Consequence: If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
- Impact: Users are vulnerable to data interception, man-in-the-middle attacks, and malicious activities.
- Recommendation: Purchase or generate a proper SSL certificate for this service.





Description: SSL Self-Guided Certificate

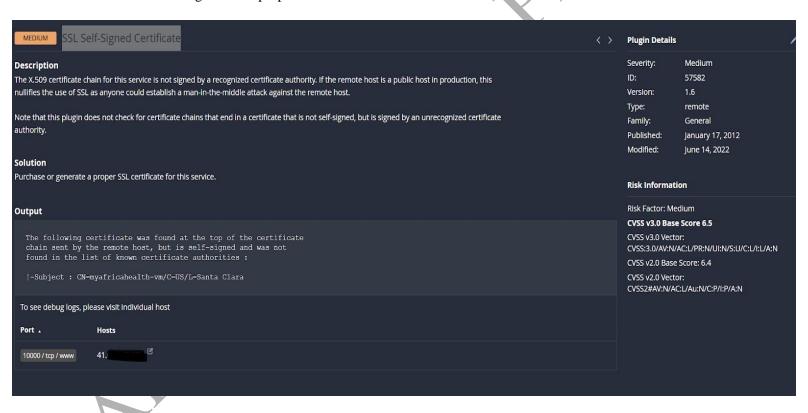
• CVE: N/A

Risk Rating: 6.5Likelihood: Medium

• Consequence: Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed but is signed by an unrecognized certificate authority.

• Impact: lack of trust and authentication

• Recommendation: Purchase or generate a proper SSL certificate for this service.





System IP: 102.

Service Enumeration

Server IP Address	Ports Open	Observations
102.	TCP: 22/53/80	
	UDP:	

Vulnerability #1

• Description: Weak MAC Algorithm (s) Supported (SSH)

• CVE: N/A

• Risk Rating: 2.6

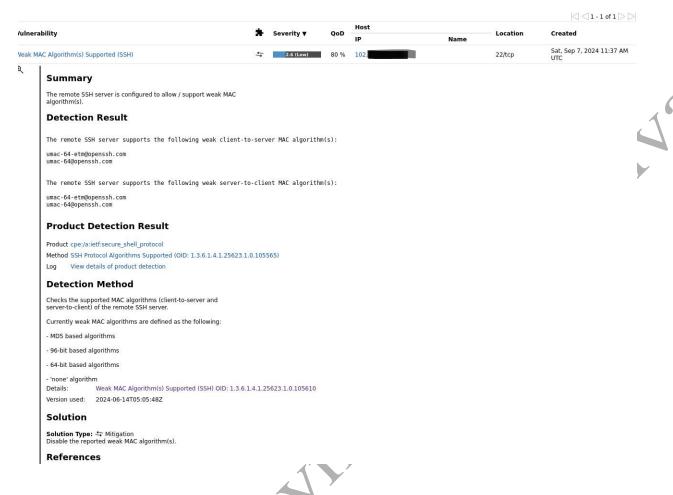
Likelihood: Low

• Consequence: Data Integrity Compromise, Authentication Bypass, Replay Attacks, Man-In-The-Middle Attacks, Cryptographic Attacks

• Impact: Financial Loss, Reputation Damage, Impact on Encrypted Communications, and Non-Compliance with Security Standards

• Recommendation: Disable the reported weak MAC algorithm





Appendix: Informational Vulnerability Assessments

HTTP ServerType and Version
HyperText Transfer Protocol (HTTP) Information
HSTS Missing from HTTPS Server
SSL Certificatre Expiry – Future Expiry (10/19/24)
SSL Certificate Information



SSL Cipher Suites Supported

SSL Perfect Forward Secrecy Cipher Suites Supported

SSL/TLS Versions Supported

SSL/TLS Recommended Cipher Suites

TLS Next Protocol Supported

Backported Security Patch Detection (SSH)

SSH Protocol Versions Supported

SSH Algorithms and Language Supported

SSH SHA-1 HMAC Algorithms Enabled

SSH Password Authentication Accepted

SSH Server Type and Version Information

TLS Version 1.2 Protocol Detection

TLS Version 1.3 Protocol Detection

Common Platform Enumeration (CPE)

Web Server Robots.txt Information Disclosure