Client Final Report Template

Infrastructure Vulnerability Project

[redacted]

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

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, [redacted] can improve its overall security and reduce the risk of cyber-attacks.

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
41.60.245.67	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.
41.60.245.67	SSL Certificate Cannot Be Trusted	Medium	Generally, means that your browser or server cannot verify the authenticity of the certificate.
41.60.245.67	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.
102.37.157.86	Missing Cookie Attribute (HTTP)	Medium	When an HTTP cookie is missing attributes, it may pose security risks or affect functionality.
102.37.157.86	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.
102.37.157.86	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.
102.37.157.213	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

- 102.37.157.86
- 41.60.245.67
- 102.37.157.213

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: 102.37.157.86

Service Enumeration

Server IP Address	Ports Open	Observations
102.37.157.86	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

NVT: Missing 'Secure' Cookie Attribute (HTTP)

ID: 1.3.6.1.4.1.25623.1.0.902661 Created: Thu, Mar 1, 2012 11:40 AM UTC Modified: Fri, Jan 12, 2024 4:12 PM UTC Owner: *(Global Object)*

Information | Preferences (0) | User Tags (0)

Summary

The remote HTTP web server / application is missing to set the
'Secure' cookie attribute for one or more sent HTTP cookie.

Scoring

CVSS Base	5.0 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Origin	N/A
CVSS Date	Thu, Mar 1, 2012 11:40 AM UTC

Insight

The flaw exists if a cookie is not using the 'Secure' cookie
attribute and is sent over a SSL/TLS connection.

This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and
subsequently allows an attacker to e.g. conduct session hijacking attacks.

Detection Method

Checks all cookies sent by the remote HTTP web server /
application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Quality of Detection: remote_analysis (70%)

Affected Software/OS

Any web application accessible via a SSL/TLS connection (HTTPS)
and at the same time also accessible over a cleartext connection (HTTP).

Solution

Solution Type: Mitigation
- Set the 'Secure' cookie attribute for any cookies that are
sent over a SSL/TLS connection

- Evaluate / do an own assessment of the security impact on the web server / application and create
an override for this result if there is none (this can't be checked automatically by this VT)

Family

Web application abuses

References

Other https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
https://owasp.org/www-community/controls/SecureCookieAttribute
https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Vulnerability #2

- 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.

NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

ID: 1.3.6.1.4.1.25623.1.0.105925 Created: Mon, Sep 1, 2014 3:00 PM UTC Modified: Fri, Jan 12, 2024 4:12 PM UTC Owner: *(Global Object)*

Information | Preferences (0) | User Tags (0)

Summary

The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Scoring

CVSS Base	5.0 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Origin	N/A
CVSS Date	Mon, Sep 1, 2014 3:00 PM UTC

Insight

The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.

This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Detection Method

Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Quality of Detection: remote_analysis (70%)

Affected Software/OS

Any web application with session handling in cookies.

Solution

Solution Type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie

- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Family

Web application abuses

References

Other https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
https://owasp.org/www-community/HttpOnly
https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Vulnerability #3

- Description: SSL/TLS: Renegotiation DOS Vulnerability
- CVE: 2011-1473; 2011-5094
- Risk Rating: 5.0
- Likelihood: 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.

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

ID: 1.3.6.1.4.1.25623.1.0.117761 | Created: Fri, Oct 29, 2021 8:24 AM UTC | Modified: Wed, Jul 24, 2024 5:06 AM UTC | Owner: *(Global Object)*

Information | Preferences *(0)* | User Tags *(0)*

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

Vulnerability #4

- 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

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com


The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com
```

Product Detection Result

Product cpe:/a:ietf:secure_shell_protocol

Method SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Log View details of product detection

Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms

- 96-bit based algorithms

- 64-bit based algorithms

- 'none' algorithm

Details: Weak MAC Algorithm(s) Supported (SSH) OID: 1.3.6.1.4.1.25623.1.0.105610

Version used: 2024-06-14T05:05:48Z

Solution

Solution Type: Mitigation
Disable the reported weak MAC algorithm(s).

References

Other https://www.rfc-editor.org/rfc/rfc6668
https://www.rfc-editor.org/rfc/rfc4253#section-6.4

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

1 - 3 of 3

System IP: 41.60.245.67

Service Enumeration

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

Vulnerability #1

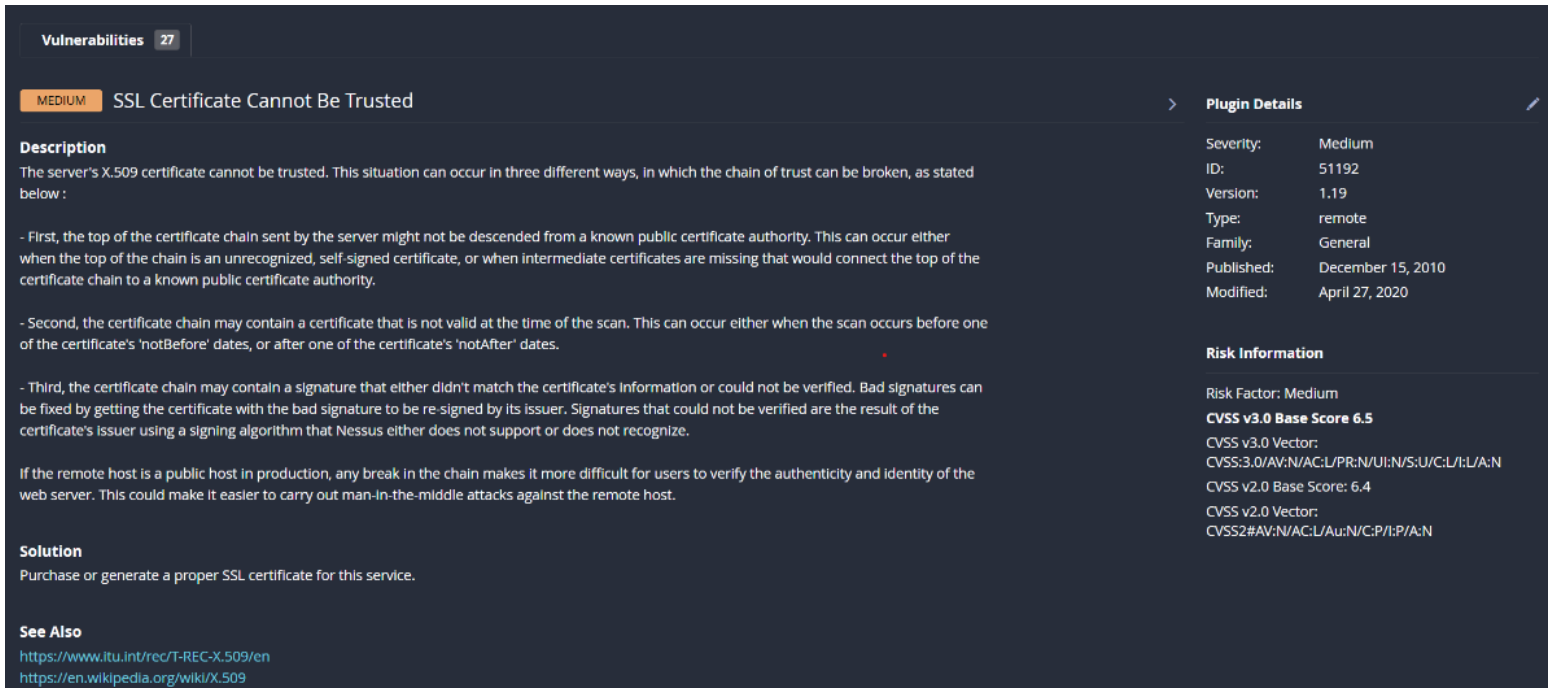
- Description: Apache HTTP Server (DOS)
- CVE: 2011-3192/2007-6750
- Risk Rating:7.8
- Likelihood: High
- Consequence: Disruption in service availability, often leading to denial of service for legitimate users, potentially affecting critical business operations and leading to loss of revenue or user 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.

```
┌──(christian㉿kali)-[~]
└─$ nmap --script vuln 41.60.245.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 17:50 PDT
Nmap scan report for 41.60.245.67
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
|     References:
|       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:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: 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/jsp/: Oracle j2ee examples
|   /dsc/: Trend Micro Data Loss Prevention Virtual Appliance
|   /reg_1.htm: Polycom IP phone
|   /adr.htm: Snom IP Phone
```

Vulnerability #2

- Description: SSL Certificate Cannot Be Trusted
- CVE: N/A
- Risk Rating: 6.5
- Likelihood: 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.



Vulnerabilities 27

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

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.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Plugin Details

Severity:	Medium
ID:	51192
Version:	1.19
Type:	remote
Family:	General
Published:	December 15, 2010
Modified:	April 27, 2020

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Vulnerability #3

- Description: SSL Self-Guided Certificate
- CVE: N/A
- Risk Rating: 6.5
- Likelihood: 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.

MEDIUM SSL Self-Signed Certificate

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

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.

Solution

Purchase or generate a proper SSL certificate for this service.

Output

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=myafricahealth-vm/C=US/L=Santa Clara
```

To see debug logs, please visit individual host

Port	Hosts
10000 / tcp / www	41.60.245.67

Plugin Details

Severity:	Medium
ID:	57582
Version:	1.6
Type:	remote
Family:	General
Published:	January 17, 2012
Modified:	June 14, 2022

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Base Score: 6.4

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

System IP: 102.37.157.213

Service Enumeration

Server IP Address	Ports Open	Observations
102.37.157.213	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

1 - 1 of 1

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	102.37.157.213		22/tcp	Sat, Sep 7, 2024 11:37 AM UTC

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com


The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com
```

Product Detection Result

Product cpe:/a:ietf:secure_shell_protocol

Method SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Log View details of product detection

Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms

- 96-bit based algorithms

- 64-bit based algorithms

- 'none' algorithm

Details: Weak MAC Algorithm(s) Supported (SSH) OID: 1.3.6.1.4.1.25623.1.0.105610

Version used: 2024-06-14T05:05:48Z

Solution

Solution Type: Mitigation
Disable the reported weak MAC algorithm(s).

References

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