

# Scratchpad Template Infrastructure Vulnerability Project

Designed to capture data and insights during the project work, which will not necessarily be included in the final client report.

# **Table of Contents**

General Information

Client Interview - Summary Report Template

Organization Information

Scope and Drivers

**Scheduling and Logistics** 

System and Infrastructure

**Additional Information** 

**Testing Exclusions** 

Nessus, NMAP and OpenVAS scan results

Nmap Findings

Nessus Findings

OpenVAS findings

**Additional Observations** 

**Preliminary Conclusions** 

False positives

**Next Steps** 

Appendix: Documenting vulnerabilities - explenation

# **General Information**

1. Date: 9/5/2024

- 2. Cyber assessor (Student) Name: Christian Stevens
- 3. Client company name:
- 4. Assessor's objectives: The objective of this project is to conduct an external, unauthenticated cybersecurity vulnerability assessment of My 1Health's Infrastructure.
- 5. Assessment Scope: Conduct a detailed vulnerability assessment of the Infrastructure: 102. ; 41. ; 102.
- 6. Tools used: Nmap, OpenVAS, and Nessus

# Client Interview - Summary Report Template

Designed to capture detailed information about an organization's network and systems infrastructure.

# Organization Information

- 1. Organization Name:
- 2. Contact Person:

# Scope and Drivers

- 1. Target Systems: 102. 41. 102.
- 2. Testing Drivers: None
- 3. Business Drivers: Find vulnerabilities that could cause potential damage.

# Scheduling and Logistics

- Start Date: 8/21/2024
   End Date: 9/7/2024
- 3. **Expected Duration:** Several hours
- 4. Outside Working Hours: None but preferred in the mornings

# System and Infrastructure

- 1. Critical Systems on Target IP Addresses: (Yes/No, if yes, list systems)
- 2. Public IP Addresses: (List all public IP addresses or ranges)
- 3. **Cloud Environment:** (AWS, Microsoft Azure, IBM, GCP, Other Webhost, Private Cloud, On-Premise)
- 4. **Private IP Addresses:** (Optional, only if conducting an Internal Vulnerability Assessment)
- 5. **Company Domain Names:** (List all domain names associated with target systems)

# Additional Information

- 1. **Known Vulnerabilities:** (List any known vulnerabilities in target systems)
- 2. **Security Documentation:** (Links to relevant security policies or architecture diagrams)

# **Testing Exclusions**

- 1. Specific systems or functionalities: (Explain why these are excluded)
- 2. Data or environments: (Explain why these are excluded)

# Nessus, NMAP and OpenVAS scan results

# Nmap Findings

- Hostname: https://insurance
- IP1: 41.
- Ports Open: 80 SSH/53 DOMAIN/80 HTTP
  - O TCP: 22/53/80
  - o UDP:
- Nmap command used: nmap –scrpit vuln 41.
- Observations: CVE-2011-3192/CVE-2007-6750
- Screenshots of scan results:

```
http-vuln-cve2011-3192:
VULNERABLE:
             VULNEABLE:
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://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 |
_https:ff: 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: |
| /imv.coreolo/. Authonication was not required
       /jmx-console/: Authentication was not required http-slowloris-check:
               VULNERABLE:
             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
    Disclosure date: 2009-09-1/
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
             /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
/jaee/examples/servlets/: Oracle j2ee examples
/j2ee/examples/servlets/: Oracle j2ee examples
/j2ee/examples/soryclets/: Oracle j2ee examples
/dsc/: Trend Micro Data Loss Prevention Virtual Appliance
/reg 1.htm: Polycom IP phone
                /reg_1.htm: Polycom IP phone
/adr.htm: Snom IP Phone
```

 Hostname:https:// https://referral

https://jms. https://patient-account.

• IP2...: 102.

• Ports Open: 53 DOMAIN/80 HTTP

TCP:53/80 UDP:

- Nmap command used: nmap –script vuln 102.
- Observations: None
- Screenshots of scan results:

- Hostname:
- IP1: 102.
- Ports Open: 80 SSH/53 DOMAIN/80 HTTP
  - O TCP: 22/53/80
  - O UDP:
- Nmap command used: nmap –script vuln 102.
- Observations: None
- Screenshots of scan results:

# Nessus Findings

All vulnerabilities (including those classified as Low):

- IP1: 102.
- Nessus Plugin ID:

• Vulnerability name: N/A

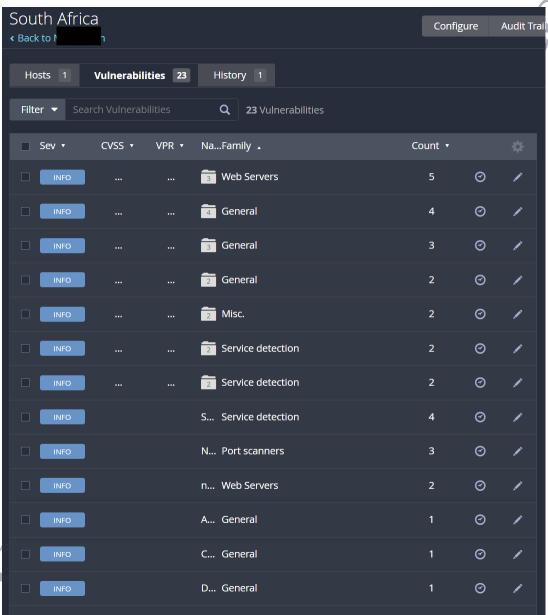
• Description: N/A

• CVE: N/A

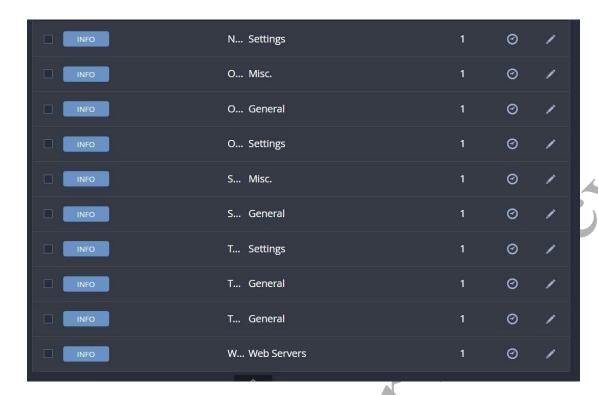
CVSS Score: N/ALikelihood: NoneConsequence: N/A

• Impact: N/A

Recommendation: N/AScreenshots of scan results:

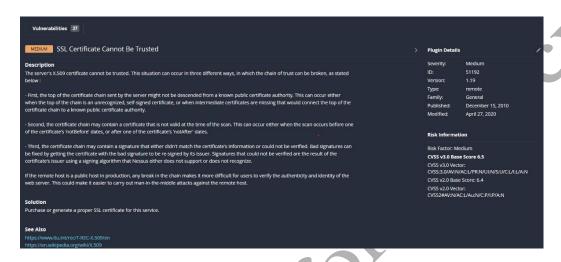




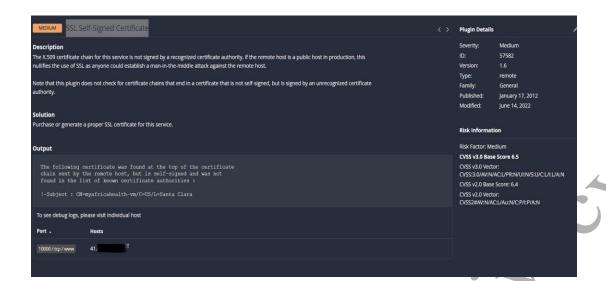


- IP2 41
- Nessus Plugin ID:
- Vulnerability name: SSL Certificate Cannot Be Trusted
- Description: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:
  - First, the top of the certificate chain 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.
- CVE: N/A
- CVSS Score: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
- Screenshots of scan results:



- IP2: 41.
- Nessus Plugin ID:
- Vulnerability Name: SSL Self-Guided 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.
- CVE: None
- CVSS Score: 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.
- Screenshots of scan results:



• IP3: 102.

• Nessus Plugin ID:

• Vulnerability name: N/A

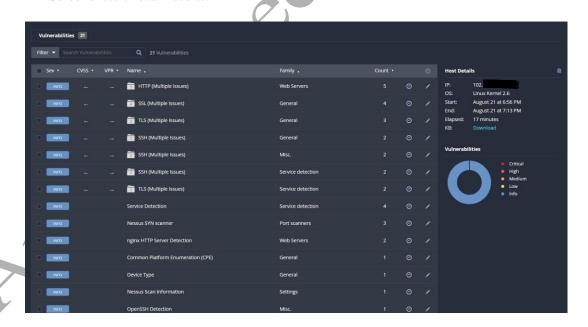
Description: N/A

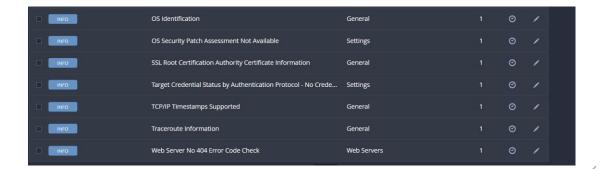
CVE: N/A

CVSS Score: N/ALikelihood: N/AConsequence: None

Impact: None

Recommendation: NoneScreenshots of scan results:





# "Informational" findings (list)

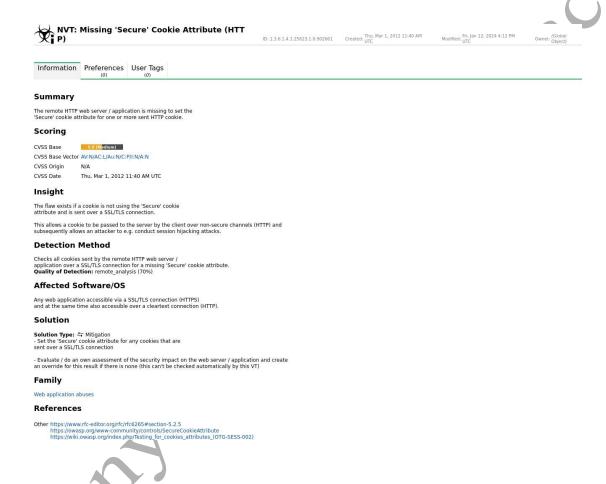
- HTTP ServerType and Version
- HyperText Transfer Protocol (HTTP) Information
- HSTS Missing from HTTPS Server
- SSL Certificatre Expiry Future Expiry (10/19/24)
- SSL Certificate Information
- SSL Cipher Suites Supported
- SSL Perfect Forward Secrecy Cipher Suites Supported
- SSL/TLS Versions Supported
- 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)

# OpenVAS findings

All vulnerabilities (including those classified as Low):

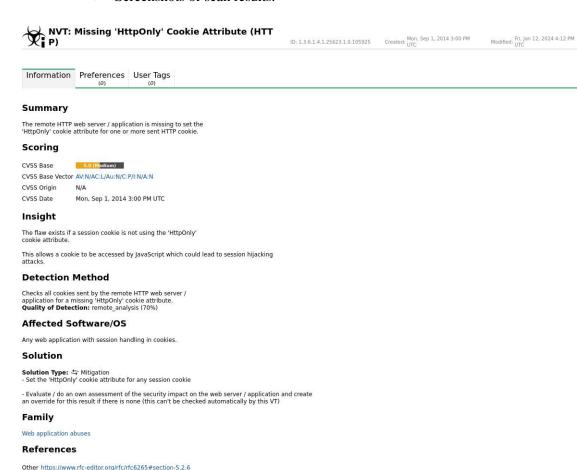
- IP1: 102.
- OpenVAS Plugin ID:
- Vulnerability name: Missing Secure Cookie Attribute (HTTP)
- Description: The remote HTTP web server / application is missing to set 'Secure' cookie attribute for one or more sent HTTP cookie

- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:



- IP1: 102.
- OpenVAS Plugin ID:
- Vulnerability name: Missing 'HTTPOnly' Cookie Attribute
- Description: The remote HTTP web server / application is missing to set 'HTTPOnly' cookie attribute for one or more sent HTTP cookie
- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:

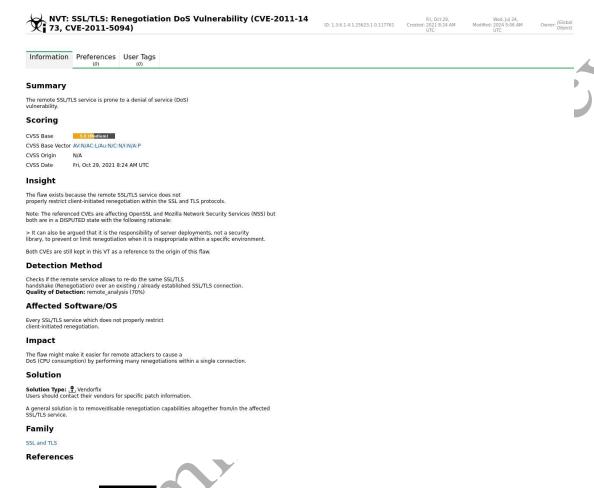


- IP1: 102.
- OpenVAS Plugin ID:

https://owasp.org/www-community/HttpOnly https://wiki.owasp.org/index.php/Testing\_for\_cookies\_attributes\_(OTG-SESS-002)

- Vulnerability Name: SSL/TLS: Renegotiation DOS Vulnerability
- Description: The remote SSL/TLS service is prone to denial of service (DOS) vulnerability
- CVE: 2011-1473; 2011-5094
- OpenVAS 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.
- Screenshots of scan results:

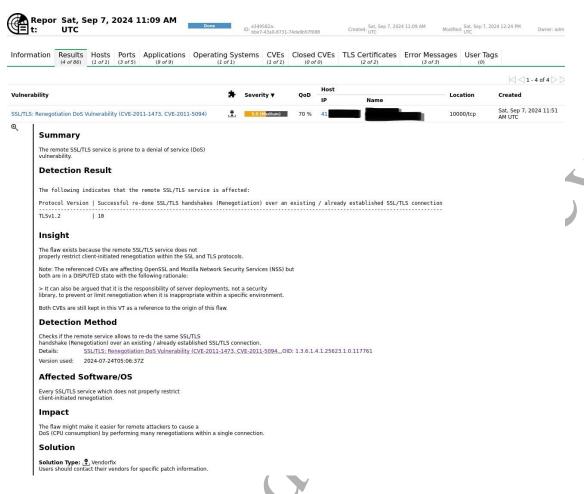


- IP1: 102.
- OpenVAS Plugin ID:
- Vulnerability name: Weak MAC Algorithm (s) Supported (SSH)
- Description: The remote server is configured to allow / support weak MAC algorithms
- CVE: N/A
- OpenVAS Risk Rating: 2.6
- Likelihood: Low
- Consequence: Data Integrity Compromise, Authentication Bypass, 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
- Screenshots of scan results:

# 0 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): **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 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=

| | | | 1 - 3 of 3 | > |

- IP1: 41.
- OpenVAS Plugin ID:
- Vulnerability name: SSL/TLS: Renegotiation DOS Vulnerability
- Description: The remote SSL/TLS service is prone to denial of service (DOS) vulnerability
- CVE: 2011-1473; 2011-5094
- OpenVAS 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.
- Screenshots of scan results:



- IP2: 41.
- OpenVAS Plugin ID:
- Vulnerability name: Missing (HTTPOnly' Cookie Attribute
- Description: The remote HTTP web server / application is missing to set 'HTTPOnly' cookie attribute for one or more sent HTTP cookie
- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:

Q

### Summary

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

### **Detection Result**

The cookie(s):

Set-Cookie: XSRFTOKEN-eyJpdi16ItpKRmRtbDl0YWswN01naHEyaDRYSXc9PSIsInZhbHVlIjoiWERlZ1Bhc2hwek1VKzk35jlVVX\SUUxmV2NpTEpnNEtKTnNhTnZQTER5Z1QrejI0Y084c29aUkx6NGRzN0c2TUF
VUXd2MZFUPHPR2SkFacxZiMng2RGFkZ6hy0XU0anJyWksvZUVuY25ya0pxZTFJNHFad2NrZ600dnVmT5tEZjgiLCJYYWM10iJhMON100FmZTUyNDdKYjYzMOdhZDEzNjAyYzAyYzEZWGM00TA3YTIZ
MZVK0DJmZmE10TJKYmUwY2EyNTkzN2U0IiwidGFnIjoiIn0%3D; expires=Sat, 07 Sep 2024 13:15:08 GMT; Max-Age=\*\*\*replaced\*\*\*; path=/; secure; samesite=lax

is/are missing the "HttpOnly" cookie attribute.

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.

Missing 'HttpOnly' Cookie Attribute (HTTP) OID: 1.3.6.1.4.1.25623.1.0.105925 Details:

Version used: 2024-01-12T16:12:12Z

### Affected Software/OS

Any web application with session handling in cookies.

Solution Type: SMitigation - 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)

### References

Other https://www.rfc-editor.org/rfc/fc6265#section-5.2.6 https://owasp.org/www-community/HttpOnly https://wiki.owasp.org/index.php/Testing\_for\_cookles\_attributes\_(OTG-SESS-002)

- IP2: 41.
- OpenVAS Plugin ID:
- Vulnerability name: Missing Secure Cookie Attribute (HTTP)
- Description: The remote HTTP web server / application is missing to set 'Secure' cookie attribute for one or more sent HTTP cookie
- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:



•

## Summary

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

### **Detection Result**

The cookie(s):

Set-Cookie:

DELINONINE:
Insurance session=eyJpdi161lBFS2Z0aE005Fc2d2IyRmJ0RWdERFE9PSIsInZhbHVlIjoiRlRBZjNgZ1d5YUtCQm5jWjlrWMYyMStRSDVCYU9CV1hl0FZuNTZEc0VSRlpIUTkzUTVFTEtxTzl
30TdYU202cVFtZ0pLQTVMT055YnhEakZYZ0lUWnBLc0cy5jddbjzYLzJNR3VpSnNtc2XTclJqcmlEswhWcHF0WjdQYUNuVjQiLCJtYmM101I5NMMvTQ3ZmVjYTIXOTNIMMVJMTI3WZ1NX20YSZMZ
NTNNNGC0NDFJMzNkOGQ0YWNjZjRhZjBmMjUyYTQZMWNhIiwidGFnIjoiIn0%3D; expires=Sat, 07 Sep 2024 13:15:08 GMT; Max-Age=\*\*\*replaced\*\*\*; path=/; httponly;
samesite=Las

is/are missing the "Secure" cookie attribute.

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.

Details: Missing 'Secure' Cookie Attribute (HTTP) OID: 1.3.6.1.4.1.25623.1.0.902661

Version used: 2024-01-12T16:12:12Z

### 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 Type: SMitigation
- 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)

### 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)

- IP2: 41.
- OpenVAS Plugin ID:
- Vulnerability name: Weak MAC Algorithm (s) Supported (SSH)
- Description: The remote server is configured to allow / support weak MAC algorithms
- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:



Φ

### 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: SMitigation
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

Anniled filter anniv overrides=0 levels=hml mws=100 min nod=70 first=1 cort\_reverse=severity

1.1 of 1 D

- IP3: 102.
- OpenVAS Plugin ID:
- Vulnerability name: Weak MAC Algorithm (s) Supported (SSH)
- Description: The remote server is configured to allow / support weak MAC algorithms
- CVE: N/A
- OpenVAS 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
- Screenshots of scan results:



 ${<\!\!\!\!<}$  1 - 1 of 1  ${>}$   ${>}$ 

(ulman)	-billion	-	Severity ▼	0-0	Host		Location	Created
/ulnerability		1.7	Seventy ¥	QoD	IP	Name		
Veak MAC Algorithm(s) Supported (SSH)		4	2.6 (Low)	80 %	102		22/tcp	Sat, Sep 7, 2024 11:37 AM UTC
Q.	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):

### **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

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

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

### Solution

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

# References

# "Informational" findings (list)

- HTTP Server type and version
- Traceroute
- SSL/TLS: Safe/Secure Renegotiation Support Status
- SSL/TLS: Untrusted Certificate Detection
- SSH Server type and version
- MariaDB/Oracle MySQL Detection

# **Additional Observations**

None



# **Preliminary Conclusions**

Nothing critical and can be solved easily.

# False positives

• Identify scan results that do not indicate a vulnerability risk. Explain how you concluded that there is no risk.

# **Next Steps**

- Report findings and compare notes with team
- Finalize the presentation to the client

# Appendix: Documenting vulnerabilities - explanation

- **Vulnerability**: Enter the descriptive name assigned to the vulnerability by the testing tool (Nessus, OpenVas, etc.) This name should provide a clear understanding of the issue.
- **Description**: Provide a brief description of the vulnerability. This information can often be found in the details section of the testing tool's output. The description should explain what the vulnerability is and how it can be exploited.
- **Risk Rating:** Record the overall risk score assigned by the testing tool. This score typically combines the likelihood and consequence of the vulnerability
- **Likelihood:** In this section, students should **estimate** the likelihood of the vulnerability being exploited. They can consider factors such as:
  - a. **Prevalence of exploit code:** Is there readily available exploit code for this vulnerability?
  - b. Exploit difficulty: How technically challenging is it to exploit this vulnerability?
  - c. Value of the target: Is your system or data a high-value target for attackers?
  - d. **Patch availability:** Is a patch available to fix the vulnerability? Students should use their understanding of the vulnerability and the environment to make an informed judgment about the likelihood of exploitation.
- **Consequence:** In this section, students should analyze the **potential consequences** of exploiting the vulnerability. They can consider the same factors mentioned for Impact, but with a focus on the severity of the potential damage:
  - a. Confidentiality: What sensitive data could be exposed if exploited?
  - b. **Integrity:** How critical are the systems or data that could be compromised?
  - c. **Availability:** What would be the impact of a system or service outage?

- d. Financial Loss: Could the vulnerability lead to significant financial losses? By considering these factors, students can assess the potential severity of the consequences if the vulnerability is exploited.
- CVE: Enter the unique identifier for the specific vulnerability identified by the testing tool (Nessus, OpenVas, etc.). This will typically be a code like CVE-2023-XXXX
- CVSS: Enter the CVSS score assigned by the testing tool. The CVSS score (0.0-10.0) reflects the severity of the vulnerability
- **Recommendation:** Provide recommendations for fixing the vulnerability. This may involve patching the system, disabling the affected service, or taking other steps to mitigate the risk