

VULNERABILITY REPORT OF PRACTICE WEBSITE

TEAM – 2.6 , TOPIC – MALWARE DETECTION AND CLASSIFICATION

1. Vulnerability Name: CGI Generic SQL Injection(blind)

Risk Factor: High

CWE: 20, 77, 89, 91, 203, 643, 713, 722, 727, 751, 801, 810, 928, 929

OSWAP CATEGORY: A03:2021- Injection

DESCRIPTION: By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

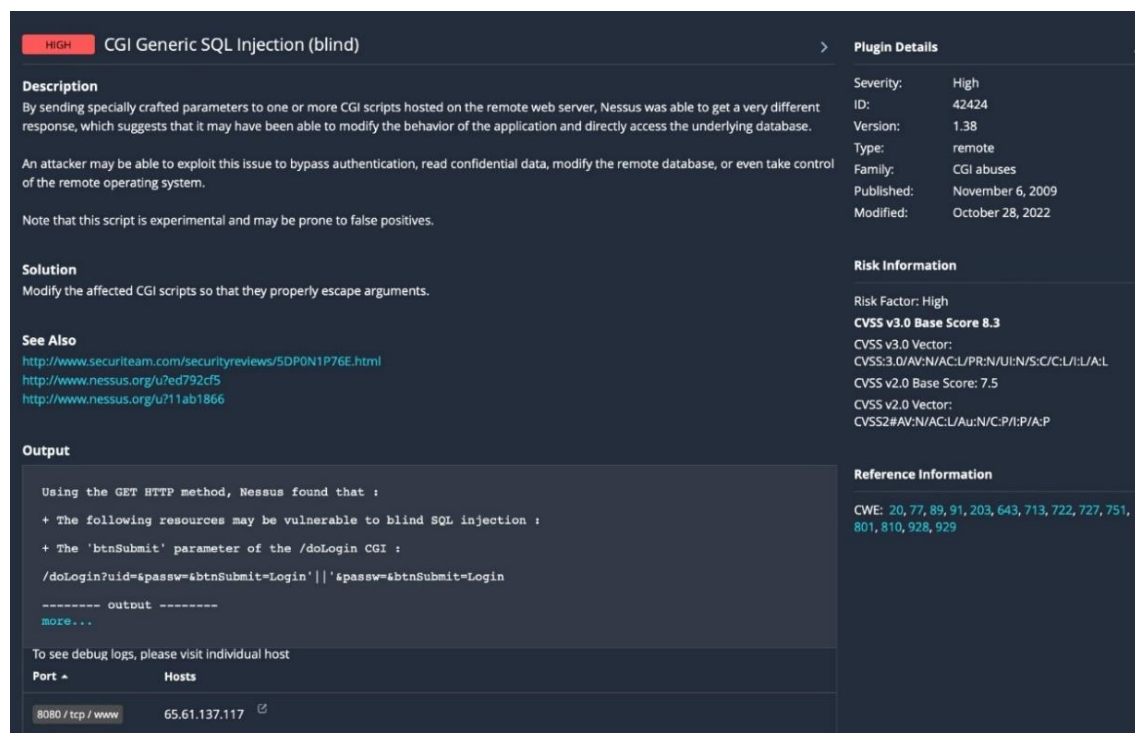
Note that this script is experimental and may be prone to false positives.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker could exploit this vulnerability to:

- Bypass authentication and gain access to sensitive data, such as customer records, financial information, or trade secrets.
- Modify or delete data in the database, which could disrupt business operations or lead to financial losses.
- Take control of the web server or underlying operating system, which could allow them to launch further attacks or disrupt the business's online operations.

Recommendation: Modify the affected CGI scripts so that they properly escape arguments.



The screenshot displays a Nessus vulnerability report for 'CGI Generic SQL Injection (blind)'. The report is categorized as 'HIGH' severity. The description states that Nessus found a vulnerability where specially crafted parameters could be used to access the underlying database. The solution is to modify the affected CGI scripts to properly escape arguments. The 'See Also' section provides links to related security reviews and Nessus advisories. The 'Output' section shows the specific parameters and the resulting database response. The 'Risk Information' section includes the CVSS v3.0 Base Score of 8.3 and the v2.0 Base Score of 7.5. The 'Reference Information' section lists the associated CWEs: 20, 77, 89, 91, 203, 643, 713, 722, 727, 751, 801, 810, 928, and 929.

Port	Hosts
8080 / tcp / www	65.61.137.117

2. Vulnerability Name: CGI Generic Cookie Injection Scripting

Risk Factor: Medium

CWE: 477, 642, 715, 722

OSWAP CATEGORY: A03:2021- Injection

DESCRIPTION: The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that:

-Nessus did not check if the session fixation attack is feasible.

-This is not the only vector of session fixation.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker could exploit this vulnerability to:

- **Steal session cookies and impersonate users:-** This could allow the attacker to access users' accounts, steal sensitive data, or make unauthorized transactions.
- **Launch session fixation attacks:-** This could allow the attacker to force a victim to use a predetermined session cookie, which could allow the attacker to impersonate the victim or steal their data.
- **Inject malicious code into cookies:-** This could allow the attacker to execute arbitrary code on the victim's browser, which could lead to data theft, account takeover, or malware infection.
- **Recommendation:** Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

The screenshot displays the Nessus interface for the 'CGI Generic Cookie Injection Scripting' plugin. The interface is divided into several sections: Description, Solution, See Also, Output, Plugin Details, Risk Information, and Reference Information. The Description section explains the vulnerability and provides a note about session fixation. The Solution section advises restricting access to the vulnerable application. The See Also section lists related resources. The Output section shows the results of a POST HTTP method test, indicating that the resources may be vulnerable to cookie manipulation. The Plugin Details section provides metadata about the plugin, including its ID, version, type, family, published and modified dates. The Risk Information section shows the risk factor as Medium and the CVSS v2.0 Base Score as 4.3. The Reference Information section lists the associated CVEs: 472, 642, 715, and 722.

MEDIUM CGI Generic Cookie Injection Scripting

Description
The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.
By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.
Please note that :
- Nessus did not check if the session fixation attack is feasible.
- This is not the only vector of session fixation.

Solution
Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

See Also
https://en.wikipedia.org/wiki/Session_fixation
https://www.owasp.org/index.php/Session_Fixation
http://www.acros.si/papers/session_fixation.pdf
<http://projects.webappsec.org/w/page/13246960/Session%20Fixation>

Output
Using the POST HTTP method, Nessus found that :
+ The following resources may be vulnerable to cookie manipulation :
+ The 'query' parameter of the /search.jsp CGI :
/search.jsp [query=<script>document.cookie="testtvlb=6860;"</script>]
----- output -----
<p>No results were found for the query:

<script>document.cookie="testtvlb=6860;"</script>

Plugin Details
Severity: Medium
ID: 44136
Version: 1.20
Type: remote
Family: CGI abuses
Published: January 25, 2010
Modified: April 11, 2022

Risk Information
Risk Factor: Medium
CVSS v2.0 Base Score: 4.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information
CVE: 472, 642, 715, 722

3. Vulnerability Name: CGI Generic HTML Injection(quick test)

Risk Factor: Medium

CWE: 80, 86

OSWAP CATEGORY: A03:2021- Injection

DESCRIPTION: The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks:

-IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing attacks.

-XSS are extensively tested by four other scripts.

-Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker could exploit this vulnerability to:

- **Inject malicious HTML into web pages:-** This could allow the attacker to deface the website, redirect users to malicious websites, or steal their data.
- **Launch cross-site scripting (XSS) attacks:-** This could allow the attacker to steal session cookies, hijack user accounts, or execute arbitrary code on the victim's browser.
- **Phish users:-** The attacker could inject malicious HTML into web pages to create phishing forms that look like legitimate login forms. If a user enters their credentials into a phishing form, the attacker can steal them.

Recommendation: Either restrict access to the vulnerable application or contact the vendor for an update.

MEDIUM CGI Generic HTML Injections (quick test)

Description
The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks:

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.
- XSS are extensively tested by four other scripts.
- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

Solution
Either restrict access to the vulnerable application or contact the vendor for an update.

See Also
<http://www.nessus.org/u7602759bc>

Output

```
Using the POST HTTP method, Nessus found that :  
+ The following resources may be vulnerable to HTML injection :  
+ The 'content' parameter of the /index.jsp CGI :  
/index.jsp [content=<<<<"bchjuv%20>>>]  
----- output -----  
BOGE...
```

To see debug logs, please visit individual host

Port **Hosts**

8080 / tcp / www 65.61.137.117

Plugin Details

Severity: Medium
ID: 49067
Version: 1.16
Type: remote
Family: CGI abuses : XSS
Published: September 1, 2010
Modified: January 19, 2021

Risk Information

Risk Factor: Medium
CVSS v2.0 Base Score: 4.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE: 80, 86

4. Vulnerability Name: CGI Generic XSS(quick test)

Risk Factor: Medium

CWE: 20, 74, 79, 80, 81, 83, 86, 116, 442, 692, 712, 722, 725, 751, 801, 811, 928, 931

OSWAP CATEGORY: A03:2021- Injection and A08:2021- Software and Data Integrity Failures

DESCRIPTION: By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Note that this script is experimental and may be prone to false positives.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker could exploit this vulnerability to:

- **Inject malicious HTML into web pages:-** This could allow the attacker to deface the website, redirect users to malicious websites, or steal their data.
- **Launch cross-site scripting (XSS) attacks:-** This could allow the attacker to steal session cookies, hijack user accounts, or execute arbitrary code on the victim's browser.
- **Phish users:-** The attacker could inject malicious HTML into web pages to create phishing forms that look like legitimate login forms. If a user enters their credentials into a phishing form, the attacker can steal them.

Recommendation: Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

MEDIUM

CGI Generic XSS (quick test)

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non persistent' or 'reflected'.

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent
<http://www.nessus.org/u?ea9a0369>
<http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>

Output

Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'content' parameter of the /index.jsp CGI :

```
/index.jsp [content="<<object type="text/html" data="http://www.example.com/include.html"></object>]
```

more...

To see debug logs, please visit individual host

Port ^	Hosts
8080 / tcp / www	65.61.137.117

Plugin Details

Severity: Medium

ID: 39466

Version: 1.45

Type: remote

Family: CGI abuses : XSS

Published: June 19, 2009

Modified: April 11, 2022

Risk Information

Risk Factor: Medium

CVSS v2.0 Base Score: 4.3

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

Reference Information

CWE: 20, 74, 79, 80, 81, 83, 86, 116, 442, 692, 712, 722, 725, 751, 801, 811, 928, 931

5. Vulnerability Name: Web Application Potentially Vulnerable to Clickjacking

Risk Factor: Medium

CWE: 693

OSWAP CATEGORY: A05:2021- Security Misconfiguration

DESCRIPTION: The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker could exploit this vulnerability to:

- Trick users into clicking on malicious buttons or links, such as fake login buttons or phishing links.
- Steal sensitive data, such as credit card information or login credentials.
- Make unauthorized transactions on the user's account.
- Launch denial-of-service attacks by flooding the victim's browser with requests.

Recommendation: Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

The screenshot shows a Nessus scan result for a vulnerability titled "Web Application Potentially Vulnerable to Clickjacking". The severity is "Medium". The description explains that the remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. The description also mentions that X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. A note states that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions. The solution is to return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags. The 'See Also' section lists links to Nessus.org, OWASP.org, and Wikipedia. The 'Output' section shows a sample output: "The following pages do not use a clickjacking mitigation response header and contain a clickable event :". The 'Plugin Details' section on the right shows: Severity: Medium, ID: 85582, Version: \$Revision: 1.7 \$, Type: remote, Family: Web Servers, Published: August 22, 2015, Modified: May 16, 2017. The 'Risk Information' section shows: Risk Factor: Medium, CVSS v2.0 Base Score: 4.3, CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N. The 'Reference Information' section shows: CWE: 693.

Web Application Potentially Vulnerable to Clickjacking	
Description	Plugin Details
The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.	Severity: Medium
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.	ID: 85582
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.	Version: \$Revision: 1.7 \$
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.	Type: remote
Solution	Family: Web Servers
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.	Published: August 22, 2015
See Also	Modified: May 16, 2017
http://www.nessus.org/u7399b1f56	Risk Information
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet	Risk Factor: Medium
https://en.wikipedia.org/wiki/Clickjacking	CVSS v2.0 Base Score: 4.3
Output	CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N
The following pages do not use a clickjacking mitigation response header and contain a clickable event :	Reference Information
	CWE: 693

6. Vulnerability Name: TLS Version 1.0 Protocol Detection

Risk Factor: Medium

CWE: 327

OSWAP CATEGORY: A02:2021-Cryptographic Failures

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.

Vulnerability Path: <http://testfire.net/>

Business Impact: The business impact of TLS Version 1.0 Protocol Detection can be significant, depending on the nature of the business and the types of data that are being transmitted.

Potential business impacts:

- Data breaches: Attackers can exploit vulnerabilities in TLS 1.0 to intercept and decrypt traffic, including sensitive data such as passwords, credit card numbers, and personal information. This could lead to data breaches that could damage a company's reputation and result in financial losses.
- Compliance violations: Many industries, such as healthcare and finance, have regulations that require companies to use secure encryption protocols. Failure to comply with these regulations could result in fines, penalties, and other legal consequences.
- Loss of customer trust: Customers are increasingly aware of the importance of cybersecurity. If they learn that a company is using outdated and insecure encryption protocols, they may lose trust in that company and take their business elsewhere.

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

The screenshot displays a vulnerability scanner interface with a dark theme. The main section is titled 'MEDIUM TLS Version 1.0 Protocol Detection'. It includes a 'Description' section with text about TLS 1.0 flaws and a 'Solution' section recommending enabling TLS 1.2 and 1.3. Below this is a 'See Also' link and an 'Output' section showing a message: 'TLSv1 is enabled and the server supports at least one cipher.' To the right, a 'Plugin Details' sidebar lists metadata: Severity (Medium), ID (104743), Version (1.10), Type (remote), Family (Service detection), Published (November 22, 2017), and Modified (April 19, 2023). Further down, 'Risk Information' shows a Risk Factor of Medium and CVSS scores (v3.0 Base Score 6.5, v2.0 Base Score 6.1). 'Vulnerability Information' indicates Asset Inventory is True. At the bottom, 'Reference Information' lists the CWE as 327. A table at the bottom left shows the scan output for port 443 on host 65.61.137.117.

Port	Hosts
443 / http / www	65.61.137.117

7. Vulnerability Name: TLS Version 1.1 Protocol Deprecated

Risk Factor: Medium

CWE: 327

OSWAP CATEGORY: A02:2021-Cryptographic Failures

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.

Vulnerability Path: <http://testfire.net/>

Business Impact: The business impact of TLS Version 1.1 Protocol Deprecated can be similar to the business impact of TLS Version 1.0 Protocol Detection, as described in my previous response.

Potential business impacts:

- Data breaches: Attackers can exploit vulnerabilities in TLS 1.0 to intercept and decrypt traffic, including sensitive data such as passwords, credit card numbers, and personal information. This could lead to data breaches that could damage a company's reputation and result in financial losses.
- Compliance violations: Many industries, such as healthcare and finance, have regulations that require companies to use secure encryption protocols. Failure to comply with these regulations could result in fines, penalties, and other legal consequences.
- Loss of customer trust: Customers are increasingly aware of the importance of cybersecurity. If they learn that a company is using outdated and insecure encryption protocols, they may lose trust in that company and take their business elsewhere.

Recommendation: Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.1.

MEDIUM

TLS Version 1.1 Protocol Deprecated

< >

Plugin Details

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.

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

See Also
<https://datatracker.ietf.org/doc/html/rfc8996>
<http://www.nessus.org/u?c8ae820d>

Output

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

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	65.61.137.117

Risk Information

Severity: Medium
ID: 157288
Version: 1.3
Type: remote
Family: Service detection
Published: April 4, 2022
Modified: April 19, 2023

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:U/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

Vulnerability Information

Asset Inventory: True

Reference Information

CWE: 327

8. Vulnerability Name: SSL/TLS Diffie-Hellman Modulus<=1024 Bits(Logjam)

Risk Factor: Low

CVE: CVE-2015-4000

DESCRIPTION: The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Vulnerability Path: <http://testfire.net/>

LOW

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

< >

Plugin Details

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

See Also

<https://weakdh.org/>

Output

```
Vulnerable connection combinations :

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_256_GCM_SHA384
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

more...
```

To see debug logs, please visit individual host

Port ^	Hosts
443 / tcp / www	65.61.137.117

Severity: Low

ID: 83875

Version: 1.40

Type: remote

Family: Misc.

Published: May 28, 2015

Modified: December 5, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Very High

CVSSv3 Impact Score: 1.4

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.5

Risk Factor: Low

CVSS v3.0 Base Score 3.7

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

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 3.2

CVSS v2.0 Base Score: 2.6

CVSS v2.0 Temporal Score: 1.9

CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

```
SSL/TLS version : TLSv1.0
Cipher suite : TLS1_256_GCM_SHA384
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

more...
```

To see debug logs, please visit individual host

Port ^	Hosts
443 / tcp / www	65.61.137.117

CVSSv3 Impact Score: 1.4

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.5

Risk Factor: Low

CVSS v3.0 Base Score 3.7

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

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 3.2

CVSS v2.0 Base Score: 2.6

CVSS v2.0 Temporal Score: 1.9

CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Vulnerability Information

CPE: cpe:/a:openssl:openssl

Exploit Ease: No known exploits are available

Vulnerability Pub Date: May 20, 2015

In the news: true

Reference Information

BID: 74733

CEA-ID: CEA-2021-0004

CVE: CVE-2015-4000

9. Vulnerability Name: Web Server Transmits Cleartext Credentials

Risk Factor: Low

CWE: 522, 523, 718, 724, 928, 930

OSWAP CATEGORY: A02:2021- Cryptographic Failures

DESCRIPTION: The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Vulnerability Path: <http://testfire.net/>

Business Impact: An attacker eavesdropping on the traffic between a web browser and a server could obtain the logins and passwords of valid users. This could allow the attacker to:

- Gain access to user accounts, including sensitive data such as credit card information, personal information, or financial data.
- Launch denial-of-service attacks by flooding the victim's account with requests.
- Impersonate users to commit fraud or other malicious activities.

Recommendation: Make sure that every sensitive form transmits content over HTTPS.

LOW Web Server Transmits Cleartext Credentials		Plugin Details
Description The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.		Severity: Low ID: 26194 Version: \$Revision: 1.17 \$ Type: remote Family: Web Servers Published: September 28, 2007 Modified: November 29, 2016
Solution Make sure that every sensitive form transmits content over HTTPS.		Risk Information Risk Factor: Low CVSS v2.0 Base Score: 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N
Output Page : /login.jsp Destination Page: /doLogin To see debug logs, please visit individual host		Reference Information CWE: 522, 523, 718, 724, 928, 930
Port ^	Hosts	
8080 / tcp / www	65.61.137.117	

10. Vulnerability Name: Web Server Allows Password Auto-Completion

Risk Factor: Low

OSWAP CATEGORY: A07:2021- Identification and Authentication Failures

DESCRIPTION: The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Vulnerability Path: <http://testfire.net/>

Business Impact: The business impact of a web server allowing password auto-completion is low, but it is still a good practice to mitigate this risk. If a user's browser is compromised, an attacker could gain access to their saved credentials and use them to access the web server.

Recommendation: Add the attribute 'autocomplete=off' to these fields to prevent browsers from catching credentials.

LOW

Web Server Allows Password Auto-Completion

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Output

Page : /login.jsp
Destination Page: /doLogin

To see debug logs, please visit individual host

Port ^

Hosts

8080 / tcp / www65.61.137.117

Plugin Details

Severity:Low

ID:42057

Version:1.11

Type:remote

Family:Web Servers

Published:October 7, 2009

Modified:July 17, 2023

Risk Information

Risk Factor: Low