Tenable.io Report

Tenable.io Report

Thu, 15 Jun 2023 18:31:07 UTC

Table Of Contents

Vulnerabilities By Host 3
[redacted] 4
Assets Summary (Executive) 22
[redacted] 23

Vulnerabilities By Host

workbe.agroprime.com

Scan Information

Start time: 2023/06/15 18:03

End time: 2023/06/15 18:31

Host Information

DNS Name: [redacted]

OS: Microsoft Windows

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	26	26

Results Details

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

N/A

Risk Factor

None

References

XREF I[redacted]31

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2000/01/04, Modification date: 2020/10/30

Ports

[redacted] **(TCP/1221) Vulnerability State: Active**

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 1999/11/27, Modification date: 2023/05/03

Ports

[redacted] (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 172.16.52.198 to 52.171.56.110 :
1[redacted]52.198
17[redacted]29
2[redacted]13
240[redacted]
5[redacted]10

Hop Count: 4
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2000/04/28, Modification date: 2022/06/17

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The following title tag will be used :
Agroprime
```

[redacted] (TCP/1221) Vulnerability State: Active

```
Unfortunately, Nessus has been unable to find a way to recognize this
page so some CGI-related checks have been disabled.
```

[redacted] (TCP/80) Vulnerability State: Active

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http:/[redacted]/Owjj[redacted]n3.html
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

[redacted]CP/443) Vulnerability State: Active

```
 Subject Name:

Common Name: *[redacted].com

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: GoDaddy.com, Inc.
Organization Unit: http://certs.godaddy.com/repository/
Common Name: Go Daddy Secure Certificate Authority - G2

Serial Number: 77 A0 A7 22 E7 5B E2 AC

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 12 18:41:49 2022 GMT
Not Valid After: Aug 12 18:41:49 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BF C5 B3 2D 10 A6 B1 A1 33 46 A4 4E 23 96 05 E2 78 65 8E
            BE E6 2F AD E8 69 19 B4 DB 99 A5 25 95 32 BA F1 6F E0 77 BC
            10 E1 74 B8 E0 7A 69 FD 7E 43 FB E0 FC 43 37 16 C9 46 76 57
            49 2C F[redacted] 2A 4B C1 88 9D E2 C2 24 6A 4C B2 E0 1E AA 59 75
            88 C7 4A 0[redacted]9 78 54 B2 ED 50 CE 1D 54 E8 A2 AA E1 95 3F
            9D 7C 68 70 CC [redacted] 5D A7 0F 71 BD FF EA 7C 51 47 DA DA B1
            20 03 51 73 21 DF D[redacted] D2 42 A1 0B CC 84 9A F9 40 08 18
            A5 D9 CF D8 FB D1 70 7E E2 [redacted] AF E8 2F 1C EE 05 B3 89
            B6 7A BE 1A 9D 20 63 CC 2E F5 44 F[redacted] FE CE 65 64 [redacted]0 A4
            93 08 56 89 6F CA 22 95 03 AA CE FE FB 0[redacted] 13 F5 5B
            3A 8C 2A 2F 96 29 [redacted] 75 D8 88 A9 25 C0
            3C 54 E0 CA DA 03 92 5C 6E 43 7C 4E 40 B3 96 1E 33 8E 3B AF
            F6 C3 26 B5 95 42 45 C4 F9 6C 06 1A 1D 28 9C 26 B9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 13 B9 8D 3D 62 BA F7 F5 27 29 E1 0C 93 FD EA 3F B9 C9 2F
           53 5F A7 27 F9 56 76 20 A6 A0 1B 96 87 F6 BE CF E7 19 D8 7A
           FE 4F 2D 33 76 AC 79 33 99 F2 3A 5B 6D E7 2D 4E 3A 86 4F B6
           84 26 99 27 83 1B A2 2F CE BA 59 1E 08 E5 B7 8D 35 6E 56 10
           73 E2 7E 4A 0C 43 CA 02 D0 3F 80 21 13 8D 07 33 4A E6 7C 4A
           4F 63 36 B5 1F EE 1D 0C 7F 26 90 56 59 0E 0D D2 AE 98 7D DD
           CC ED 33 56 A0 7B 54 BB 42 E3 5C 84 D8 7F D7 52 93 4B 8B EA
           0E A6 D7 21 [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2009/02/04, Modification date: 2023/05/31

Ports

[redacted] (TCP/4022) Vulnerability State: Active

Port 4022/tcp was found to be open

[redacted] (TCP/1221) Vulnerability State: Active

Port 1221/tcp was found to be open

[redacted] (TCP/80) Vulnerability State: Active

Port 80/tcp was found to be open

[redacted] (TCP/443) Vulnerability State: Active

Port 443/tcp was found to be open

[redacted] (TCP/4024) Vulnerability State: Active

Port 4024/tcp was found to be open

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2003/12/09, Modification date: 2022/03/09

Ports

[redacted]CP/0) Vulnerability State: Active

```
Remote operating system : Microsoft Windows
Confidence level : 70
Method : HTTP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-HTTPAPI/2.0

SinFP:!:
   P1:B11113:F0x12:W[redacted]4ffff:M1440:
   P2:B11113:F0x12:W6553[redacted]0affffffff44454144:M1440:
   P3:B00000:F0x00:W0:O0:M0
   P4:190502_7_p=80R
SSLcert:!:i/CN:Go Daddy Secure Certificate Authority - G2i/O:GoDaddy.com, Inc.i/OU:http://
certs.godaddy.com/repository/s/CN:*[redacted]com
3b4d1a508[redacted]008c3a3afe8311350db
```

```
The remote host is running Microsoft Windows
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2005/08/26, Modification date: 2023/04/27

Ports

[redacted] (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306150801
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : amzn2-aarch64
Scan type : Normal
Scan name : Workbe4
Scan policy used : Basic Network Scan
Scanner IP : tenable.io Scanner
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 333.428 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/6/15 18:04 UTC
Scan duration : 1600 sec
```

```
Scan for malware : no
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2006/06/05, Modification date: 2022/07/25

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2007/08/19, Modification date: 2023/03/29

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
A TLSv1.2 server answered on this port.


A web server is running on this port through TLSv1.2.
```

[redacted] (TCP/1221) Vulnerability State: Active

```
A web server is running on this port.
```

[redacted] (TCP/80) Vulnerability State: Active

```
A web server is running on this port.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2007/01/30, Modification date: 2019/11/22

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

  Content-Length: 21431
  Connection: close
  Content-Type: text/html
  Date: Thu, 15 Jun 2023 18:18:35 GMT
  Accept-Ranges: bytes
  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
  ETag: "0d6ebd209ed91:0"
  Last-Modified: Tue, 13 Jun 2023 14:10:36 GMT
  X-Frame-Options: DENY
  X-XSS-Protection: 1; mode=block
  X-Content-Type-Options: nosniff
  Strict-Transport-Security: max-age=31536000
```

```
  Content-Security-Policy: default-src 'self'; script-src 'self' maps.googleapis.com 'unsafe-
inline' 'unsafe-eval' data:; style-src 'self' fonts.googleapis.com fonts.gstatic.com 'unsafe-
inline' 'unsafe-eval' data:; img-src 'self' data: blob: agroprime.blob.core.windows.net
 *.google.com maps.gstatic.com; font-src 'self' fonts.gstatic.com data: fonts.googleapis.com;
 connect-src 'self' *.agroprime.com agroprime-api-test.azurewebsites.net agroprime-api-
dev.azurewebsites.net wss://a[redacted]wss://a[redacted]t.azurewebsites.net wss://
a[redacted]dev.azurewebsites.net maps.googleapis.com; object-src 'none'; frame-ancestors
 'none'; block-all-mixed-content; upgrade-insecure-requests;

Response Body :

<!DOCTYPE html><html lang="en"><head><link rel="preconnect" href="https://fonts.gstatic.com"
 crossorigin="">
    <meta charset="utf-8">
    <title[redacted]/title>
    <base href="/">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-
scalable=0">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <link rel="icon" type="image/png" href="./assets/media/logo-agroprime-circle.png">

    <!-- <link id="theme-css" rel="stylesheet" type="text/css" href="assets/theme/orange/theme-
dark.css">
    <link id="layout-css" rel="stylesheet" type="text/css" [...]
```

[redacted]/80) Vulnerability State: Active

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Length: 0
  Connection: close
  Date: Thu, 15 Jun 2023 18:18:33 GMT
  Location: https:/[redacted]/

Response Body :
```

[redacted]CP/1221) Vulnerability State: Active

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Transfer-Encoding: chunked
  Content-Type: text/plain
  Server: Microsoft-HTTPAPI/2.0
  Strict-Transport-Security: max-age=31536000
  X-Frame-Options: DENY
  X-XSS-Protection: 1
  X-Content-Type-Options: nosniff
  Date: Thu, 15 Jun 2023 18:18:30 GMT
  Connection: close

Response Body :

40.74.224.176
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2007/05/16, Modification date: 2019/03/06

Ports

[redacted]CP/0) Vulnerability State: Active

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).
The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.
All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2009/11/16, Modification date: 2019/11/22

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The STS header line is :

Strict-Transport-Security: max-age=31536000
```

[redacted] (TCP/1221) Vulnerability State: Active

```
The STS header line is :

Strict-Transport-Security: max-age=31536000
```

42823 - Non-compliant Strict Transport Security (STS)

Synopsis

The remote web server implements Strict Transport Security incorrectly.

Description

The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2009/11/16, Modification date: 2014/09/19

Ports

[redacted] (TCP/1221) Vulnerability State: Active

```
The Strict-Transport-Security header must not be sent over an
unencrypted channel.
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2009/12/02, Modification date: 2020/09/04

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The SSL certificate will expire within 60 days, at
Aug 12 18:41:49 2023 GMT :

  Subject          : CN=*.agroprime.com
  Issuer           : C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://
certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
  Not valid before : Aug 12 18:41:49 2022 GMT
  Not valid after  : Aug 12 18:41:49 2023 GMT
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD
Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response.
If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2009/12/10, Modification date: 2022/04/11

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
Based on the response to an OPTIONS request :

  - HTTP methods  GET  HEAD  POST  TRACE OPTIONS are allowed on :

    /
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2010/04/21, Modification date: 2023/06/08

Ports

[redacted] (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :
```

```
cpe:/o:microsoft:windows -> Microsoft Windows
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2011/05/23, Modification date: 2022/09/09

Ports

[redacted] (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 70
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2011/12/01, Modification date: 2021/02/03

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
This port supports TLSv1.2.
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

[redacted](TCP/443) Vulnerability State: Active

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA       AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA       AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA       AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA       AES-CBC(256)
 SHA384

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
MAC
    ----------------------        ----------       ---           ----      --------------------
---
    ECDHE-RSA-[redacted]28-SHA          0xC0, 0x13       ECDH          RSA       AES-CBC(128)
SHA1
    ECDHE-RSA[redacted]56-SHA           0xC0, 0x14       ECDH          RSA       AES-CBC(256)
SHA1
    ECDH[redacted]56       0xC0, 0x27       ECDH          RSA       AES-CBC(128)
SHA256
    ECDHE-RSA[redacted]256-SHA384       0xC0, 0x28       ECDH          RSA       AES-CBC(256)
SHA384

The fields above are :

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

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2015/05/08, Modification date: 2015/05/08

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=*.agroprime.com
|-Not After : Aug 12 18:41:49 2023 GMT
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2015/07/17, Modification date: 2021/02/03

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
http/1.1
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2016/11/14, Modification date: 2018/11/15

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The following root Certification Authority certificate was found :

|-Subject            : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification
 Authority
|-Issuer             : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification
 Authority
|-Valid From         : Jun 29 17:06:20 2004 GMT
|-Valid To           : Jun 29 17:06:20 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known

to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.
Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	33065
BID	11849
XREF	CWE-310

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2016/12/08, Modification date: 2022/10/12

Ports

[redacted] (TCP/443) Vulnerability State: Active

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:06:20 2004 GMT
Valid To            : Jun 29 17:06:20 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMT
+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCAPVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/
Hd8M+eKsaA7Ugay9[redacted]BQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMYavx4A6lNf4DD
ojgC95/5Y0V4evLO[redacted]
+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZE[redacted]ihfukEHU1jPEX44dMX4/7VpkI
+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFN[redacted]yz2h/
t2oatTjMIGNBgNVHSMEgY[redacted]Nnyz2h/
t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGF
+YeAEW5p5JYXMP80kWNy[redacted]U1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7PTMozI
+gciKqdi0FuFskg5YmezT[redacted]heabIZ0KbIIOqPjCDPoQHmyW74cNxA9hi63ugyuV+I6ShHI56yDqg
+2DzZduCLzrTia2cyvk0/ZM/iZx4mERdEr/
VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5CufReYNnyicsbkqWletNw+vHX/bvZ8=
-----END CERTIFICATE-----
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2020/05/04, Modification date: 2020/05/04

Ports

[redacted](TCP/443) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
TLSv1.3:
- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256
TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384
This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Exploitable with

Metasploit, CANVAS, Core Impact

Plugin Information:

Publication date: 2022/01/20, Modification date: 2022/04/06

Ports

[redacted](TCP/443) Vulnerability State: Active

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:
```

```
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX          Auth     Encryption
 MAC
    ----------------------        ----------       ---          ----     --------------------
 ---
    ECDHE-R[redacted]S128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
 SHA1
    ECDHE[redacted]AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
 SHA1
    ECDHE-RS[redacted]28-SHA256        0xC0, 0x27       ECDH         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA[redacted]-SHA384         0xC0, 0x28       ECDH         RSA      AES-CBC(256)
 SHA384

The fields above are :

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

Assets Summary (Executive)

[redacted]

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	26	26

Details

Severity	Plugin Id	Name
Info	136318	TLS Version 1.2 Protocol Detection
Info	10863	SSL Certificate Information
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	42822	Strict Transport Security (STS) Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	11219	Nessus SYN scanner
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	25220	TCP/IP Timestamps Supported
Info	19506	Nessus Scan Information
Info	10107	HTTP Server Type and Version
Info	21643	SSL Cipher Suites Supported
Info	94761	SSL Root Certification Authority Certificate Information
Info	54615	Device Type
Info	43111	HTTP Methods Allowed (per directory)
Info	156899	SSL/TLS Recommended Cipher Suites
Info	10287	Traceroute Information
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	22964	Service Detection
Info	11936	OS Identification
Info	84821	TLS ALPN Supported Protocol Enumeration
Info	56984	SSL / TLS Versions Supported
Info	45590	Common Platform Enumeration (CPE)
Info	42823	Non-compliant Strict Transport Security (STS)
Info	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
Info	10386	Web Server No 404 Error Code Check