



# Local Vulnerability Assessment of Project

Report generated by Tenable Nessus™

Wed, 09 Apr 2025 16:11:41 EDT

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Plugin

• 51192 (1) - SSL Certificate Cannot Be Trusted.....	4
• 142960 (1) - HSTS Missing From HTTPS Server (RFC 6797).....	6
• 10107 (2) - HTTP Server Type and Version.....	8
• 10386 (2) - Web Server No 404 Error Code Check.....	9
• 11219 (2) - Nessus SYN scanner.....	11
• 24260 (2) - HyperText Transfer Protocol (HTTP) Information.....	12
• 10287 (1) - Traceroute Information.....	14
• 10863 (1) - SSL Certificate Information.....	15
• 11936 (1) - OS Identification.....	17
• 19506 (1) - Nessus Scan Information.....	18
• 21643 (1) - SSL Cipher Suites Supported.....	20
• 25220 (1) - TCP/IP Timestamps Supported.....	22
• 42981 (1) - SSL Certificate Expiry - Future Expiry.....	23
• 45590 (1) - Common Platform Enumeration (CPE).....	24
• 46180 (1) - Additional DNS Hostnames.....	25
• 54615 (1) - Device Type.....	26
• 56984 (1) - SSL / TLS Versions Supported.....	27
• 57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported.....	28
• 70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported.....	30
• 83298 (1) - SSL Certificate Chain Contains Certificates Expiring Soon.....	32
• 84502 (1) - HSTS Missing From HTTPS Server.....	33
• 84821 (1) - TLS ALPN Supported Protocol Enumeration.....	34
• 156899 (1) - SSL/TLS Recommended Cipher Suites.....	35
• 209654 (1) - OS Fingerprints Detected.....	37

---

## **Vulnerabilities by Plugin**

---

## 51192 (1) - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

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

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

---

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

---

echargestations.infinityfreeapp.com (tcp/443/www)

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :
```

```
| -Subject : CN=echargestations.infinityfreeapp.com
| -Issuer  : C=US/O=Google Trust Services/CN=WR1
```

## 142960 (1) - HSTS Missing From HTTPS Server (RFC 6797)

### Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

### Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

<https://tools.ietf.org/html/rfc6797>

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 09 Apr 2025 20:03:11 GMT
Content-Type: text/html
Content-Length: 847
Connection: close
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Cache-Control: no-cache
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

## 10107 (2) - 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 IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

echargestations.infinityfreeapp.com (tcp/80/www)

```
The remote web server type is :
```

```
openresty
```

echargestations.infinityfreeapp.com (tcp/443/www)

```
The remote web server type is :
```

```
openresty
```



## 10386 (2) - 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

### Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

### Plugin Output

echargestations.infinityfreeapp.com (tcp/80/www)

The following body tag will be used :

```
<html><script type="text/javascript" src="/aes.js" ></script><script>function
toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return
e}function toHex(){for(var d=[],d1=arguments.length&&arguments[0].constructor==Array?
arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return
e.toLowerCase()}var
a=toNumbers("f655ba9d09a112d4968c63579db590b4"),b=toNumbers("98344c2eee86c3994890592585b49f80"),c=toNumbers("519b
expires=Thu, 31-Dec-37 23:55:55 GMT; path=/"; location.href="http://
echargestations.infinityfreeapp.com/Cs4kvkbDMrKE.html?i=1";</script><noscript>This site requires
Javascript to work, please enable Javascript in your browser or use a browser with Javascript
support</noscript></body></html>
```

echargestations.infinityfreeapp.com (tcp/443/www)

The following body tag will be used :

```
<html><script type="text/javascript" src="/aes.js" ></script><script>function
toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return
e}function toHex(){for(var d=[],d1=arguments.length&&arguments[0].constructor==Array?
arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return
e.toLowerCase()}var
a=toNumbers("f655ba9d09a112d4968c63579db590b4"),b=toNumbers("98344c2eee86c3994890592585b49f80"),c=toNumbers("519b
```

```
expires=Thu, 31-Dec-37 23:55:55 GMT; path=/; location.href="https://  
echargestations.infinityfreeapp.com/Cs4kvkbDMrKE.html?i=1";</script><noscript>This site requires  
Javascript to work, please enable Javascript in your browser or use a browser with Javascript  
support</noscript></body></html
```

## 11219 (2) - 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

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

echargestations.infinityfreeapp.com (tcp/80/www)

```
Port 80/tcp was found to be open
```

echargestations.infinityfreeapp.com (tcp/443/www)

```
Port 443/tcp was found to be open
```

## 24260 (2) - 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 is enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

echargestations.infinityfreeapp.com (tcp/80/www)

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: Yes

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: openresty

Date: Wed, 09 Apr 2025 20:05:39 GMT

Content-Type: text/html

Content-Length: 846

Connection: keep-alive

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Cache-Control: no-cache

Response Body :

```
<html><body><script type="text/javascript" src="/aes.js" ></script><script>function
toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return
e}function toHex(){for(var d=[],d=1==arguments.length&&arguments[0].constructor==Array?
arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return
e.toLowerCase()}var
a=toNumbers("f655ba9d09a112d4968c63579db590b4"),b=toNumbers("98344c2eee86c3994890592585b49f80"),c=toNumbers("519b
"
```

```
expires=Thu, 31-Dec-37 23:55:55 GMT; path="/"; location.href="http://
echargestations.infinityfreeapp.com/?i=1";</script><noscript>This site requires Javascript to work,
please enable Javascript in your browser or use a browser with Javascript support</noscript></
body></html>
```

echargestations.infinityfreeapp.com (tcp/443/www)

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : yes

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: openresty

Date: Wed, 09 Apr 2025 20:05:37 GMT

Content-Type: text/html

Content-Length: 847

Connection: keep-alive

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Cache-Control: no-cache

Response Body :

```
<html><body><script type="text/javascript" src="/aes.js" ></script><script>function
toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return
e}function toHex(){for(var d=[],d=1==arguments.length&&arguments[0].constructor==Array?
arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return
e.toLowerCase()}var
a=toNumbers("f655ba9d09a112d4968c63579db590b4"),b=toNumbers("98344c2eee86c3994890592585b49f80"),c=toNumbers("519b
expires=Thu, 31-Dec-37 23:55:55 GMT; path="/"; location.href="https://
echargestations.infinityfreeapp.com/?i=1";</script><noscript>This site requires Javascript to work,
please enable Javascript in your browser or use a browser with Javascript support</noscript></
body></html>
```

## 10287 (1) - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

echargestations.infinityfreeapp.com (udp/0)

```
For your information, here is the traceroute from 10.125.221.84 to 185.27.134.34 :
10.125.221.84
10.125.255.250
129.120.214.118
129.120.255.87
10.127.192.128
208.76.224.152
74.200.180.82
74.200.180.213
209.120.144.245
141.136.108.189
?
213.251.24.101
213.251.24.102
?
185.27.134.34

Hop Count: 16
```

## 10863 (1) - 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

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

Subject Name:

Common Name: echargestations.infinityfreeapp.com

Issuer Name:

Country: US

Organization: Google Trust Services

Common Name: WR1

Serial Number: 00 F3 A6 63 E2 02 96 6C A3 0E D1 D9 3E 1E 2F 7B 32

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 06 14:05:07 2025 GMT

Not Valid After: May 07 14:05:06 2025 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 A7 D7 BE 4C 28 09 68 BC 44 55 9D 48 FE 91 2D A0 7D B4 E0  
F0 5A 55 4B E1 05 B1 B5 87 22 A2 50 0E 1B A9 6E 4F 97 D0 90  
86 D1 9E 31 B6 79 C3 17 62 07 72 16 D6 28 6E FD FE 36 CA C5  
F4 EE 03 ED A4 A8 E8 DF 61 DA 88 D2 43 0F FB 2F 54 1F 88 27  
6C 54 00 27 A6 63 A2 EF 22 21 58 1A 1F 97 EA DC F2 96 6F 26  
DA 7A 86 7F 30 AD 2A 43 7E 29 1F B2 60 5C 27 36 37 74 9A B5  
56 F7 AA F4 03 8B 66 07 34 2A CB F0 EE 91 50 A6 83 7D B9 37  
F5 38 CE FA E0 3F A4 61 38 56 6F F8 1A 41 04 7C 68 B5 A9 A0

```
8C C1 5B A4 08 94 36 D9 12 47 65 0B FA 83 2A D8 30 07 7B 59
A2 11 85 BA 0C CD 6F 1C D0 49 E6 72 D9 3F 1A F8 23 78 63 FA
21 F0 54 3A 23 56 C4 0E 06 56 15 E8 57 AD 81 8B CC 9A 9E D1
A7 D0 F6 CA 2E 39 A7 9D FF E3 8D 81 1F 7B 09 EC 60 FB 80 5D
28 4E C3 30 8C 5B 74 E0 92 13 FA 98 13 9E 4E 2F 87
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 6E 5A CB 71 AA 12 D3 29 DC 86 01 C8 C4 18 C2 FF D3 6D C2  
10 93 45 62 A9 2E A1 C4 6B 29 A9 28 BA A9 52 44 E3 6D E9 F9  
EA D4 61 E5 F5 3D 52 51 77 A2 D4 B9 79 05 E1 2E 50 06 53 30  
EC 33 E1 AA F8 19 94 BC 3B 93 9C 8E 19 3D 01 F3 22 6B 34 D2  
AE 16 11 25 81 B2 03 45 C0 6E 8E FB 1E 91 93 D2 4B 6C 8A 25  
F1 3E 67 34 3E 9E FB EB 59 0A C1 E3 AD 0B D8 38 E6 B7 D8 BB  
65 43 7E C7 18 3D 19 51 C6 30 CD 67 53 B9 3A 5A CC C0 21 5A  
EA 7B 26 09 0E B8 99 7B 0F 80 40 9B 0C 59 FB 67 DA 80 F4 A7  
F4 06 92 56 EB A0 F1 29 A4 13 5 [...]



## 11936 (1) - 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

### Plugin Information

Published: 2003/12/09, Modified: 2025/03/31

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

```
Remote operating system : Ubuntu 16.04 Linux Kernel 4.4  
Confidence level : 56  
Method : MLSinFP
```

```
The remote host is running Ubuntu 16.04 Linux Kernel 4.4
```

## 19506 (1) - 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

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202504090549
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
```

```
Scan name : Local Vulnerability Assessment of Project
Scan policy used : Advanced Scan
Scanner IP : 10.125.221.84
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 182.781 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/4/9 16:00 EDT (UTC -04:00)
Scan duration : 618 sec
Scan for malware : no
```

## 21643 (1) - 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

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

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

SSL Version : TLSv13

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
TLS_AES_128_GCM_SHA256	0x13, 0x01	-	-	AES-GCM(128)	
AEAD					
TLS_AES_256_GCM_SHA384	0x13, 0x02	-	-	AES-GCM(256)	
AEAD					
TLS_CHACHA20_POLY1305_SHA256	0x13, 0x03	-	-	ChaCha20-Poly1305(256)	
AEAD					

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---

DHE-RSA-AES-128-CCM-AEAD AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)
DHE-RSA-AES-256-CCM-AEAD AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)
RSA-AES-128-CCM-AEAD AEAD	0xC0, 0x9C	RSA	RSA	AES-CCM(128)
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)
RSA-AES-256-CCM-AEAD	0xC0, 0x9D	RSA	RSA	[...]

## 25220 (1) - 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

### Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

## 42981 (1) - 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

### Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

```
The SSL certificate will expire within 60 days, at  
May 7 14:05:06 2025 GMT :
```

```
Subject       : CN=echargestations.infinityfreeapp.com  
Issuer        : C=US, O=Google Trust Services, CN=WR1  
Not valid before : Feb 6 14:05:07 2025 GMT  
Not valid after  : May 7 14:05:06 2025 GMT
```

## 45590 (1) - 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

### Plugin Information

Published: 2010/04/21, Modified: 2025/03/13

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

The remote operating system matched the following CPE :

```
cpe:/o:linux:linux_kernel -> Linux Kernel
```



## 46180 (1) - Additional DNS Hostnames

### Synopsis

Nessus has detected potential virtual hosts.

### Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

### See Also

[https://en.wikipedia.org/wiki/Virtual\\_hosting](https://en.wikipedia.org/wiki/Virtual_hosting)

### Solution

If you want to test them, re-scan using the special vhost syntax, such as :

`www.example.com[192.0.32.10]`

### Risk Factor

None

### Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

### Plugin Output

`echargestations.infinityfreeapp.com (tcp/0)`

```
The following hostnames point to the remote host :  
- video.infinityfreeapp.com
```

## 54615 (1) - 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

### Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

```
Remote device type : unknown  
Confidence level : 56
```

## 56984 (1) - 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

### Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

```
This port supports TLSv1.3/TLSv1.2.
```

## 57041 (1) - 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/Diffie-Hellman_key_exchange)

[https://en.wikipedia.org/wiki/Perfect\\_forward\\_secrecy](https://en.wikipedia.org/wiki/Perfect_forward_secrecy)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

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
-----	-----	---	----	-----	---
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES-256-CCM-AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)	
AEAD					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					

ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA256	0x00, 0xBE	DH	RSA	Camellia-CBC [...]

## 70544 (1) - 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/docs/manmaster/man1/ciphers.html>

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

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-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)	

DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA256 SHA256	0x00, 0xBE	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA256 SHA256	0x00, 0xC4	DH	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128) [...]

## 83298 (1) - 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

### Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

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

```
| -Subject      : CN=echargestations.infinityfreeapp.com
| -Not After    : May 07 14:05:06 2025 GMT
```



## 84502 (1) - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

<https://tools.ietf.org/html/rfc6797>

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

### Plugin Output

`echargestations.infinityfreeapp.com (tcp/443/www)`

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 09 Apr 2025 20:03:11 GMT
Content-Type: text/html
Content-Length: 847
Connection: close
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Cache-Control: no-cache
```

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

## 84821 (1) - 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

### Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

### Plugin Output

echargestations.infinityfreeapp.com (tcp/443/www)

```
http/1.1
```

## 156899 (1) - 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 TLS13\_AES\_128\_GCM\_SHA256
- 0x13,0x02 TLS13\_AES\_256\_GCM\_SHA384
- 0x13,0x03 TLS13\_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

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

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

### Solution

Only enable support for recommended cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

### Plugin Output

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
-----	-----	---	----	-----	---
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES-256-CCM-AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)	
AEAD					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CAMELLIA-CBC-128	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
SHA256					
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
SHA384					
RSA-AES-128-CCM-AEAD	0xC0, 0x9C	RSA	RSA	AES-CCM(128)	
AEAD					
RSA-AES128-SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
SHA256					
RSA-AES-256-CCM-AEAD	0xC0, 0x9D	RSA	RSA	AES-CCM(256)	
AEAD					
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
SHA384					
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	
SHA1					
DHE-RSA-CAMELLIA128-SHA	0x00, 0x45	DH	RSA	Camellia-CBC(128)	
SHA1					
DHE-RSA-CAMELLIA256-SHA	0x00, 0x88	DH	RSA	Camellia-CBC(256)	
SHA1					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
SHA1					
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
SHA1					
AES128-SHA	0x00, 0x2F	RS [...]			

## 209654 (1) - OS Fingerprints Detected

### Synopsis

Multiple OS fingerprints were detected.

### Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

### Plugin Output

echargestations.infinityfreeapp.com (tcp/0)

Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4  
Confidence level : 56  
Method : MLSinFP  
Type : unknown  
Fingerprint : unknown

Remote operating system : Linux Kernel 2.x  
Confidence level : 54  
Method : SinFP  
Type : general-purpose  
Fingerprint : SinFP:  
P1:B10113:F0x12:W29200:00204ffff:M1382:  
P2:B10113:F0x12:W28960:00204ffff0402080affffff4445414401030309:M1382:  
P3:B00000:F0x00:W0:00:M0  
P4:191003\_7\_p=443R

Following fingerprints could not be used to determine OS :  
HTTP!!:Server: openresty

SSLcert!!:i/CN:WRli/O:Google Trust Servicess/CN:echargestations.infinityfreeapp.com  
2ad3ca53c542e4c115505590ac907c9b496ddadf