



**cogent company**

---

Report generated by Nessus™

Mon, 01 Jul 2024 06:03:21 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Plugin

• 54582 (1) - SMTP Service Cleartext Login Permitted.....	5
• 70658 (1) - SSH Server CBC Mode Ciphers Enabled.....	6
• 153953 (1) - SSH Weak Key Exchange Algorithms Enabled.....	8
• 11219 (13) - Nessus SYN scanner.....	10
• 22964 (6) - Service Detection.....	12
• 10863 (4) - SSL Certificate Information.....	14
• 21643 (4) - SSL Cipher Suites Supported.....	18
• 45410 (4) - SSL Certificate 'commonName' Mismatch.....	22
• 56984 (4) - SSL / TLS Versions Supported.....	24
• 57041 (4) - SSL Perfect Forward Secrecy Cipher Suites Supported.....	25
• 94761 (4) - SSL Root Certification Authority Certificate Information.....	28
• 95631 (4) - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA).....	30
• 136318 (4) - TLS Version 1.2 Protocol Detection.....	33
• 138330 (4) - TLS Version 1.3 Protocol Detection.....	34
• 156899 (4) - SSL/TLS Recommended Cipher Suites.....	35
• 10092 (1) - FTP Server Detection.....	38
• 10107 (1) - HTTP Server Type and Version.....	39
• 10185 (1) - POP Server Detection.....	40
• 10263 (1) - SMTP Server Detection.....	41
• 10267 (1) - SSH Server Type and Version Information.....	42
• 10287 (1) - Traceroute Information.....	43
• 10719 (1) - MySQL Server Detection.....	44
• 10881 (1) - SSH Protocol Versions Supported.....	45
• 11153 (1) - Service Detection (HELP Request).....	46
• 11414 (1) - IMAP Service Banner Retrieval.....	47
• 11424 (1) - WebDAV Detection.....	48
• 11936 (1) - OS Identification.....	49

• 12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution.....	51
• 19506 (1) - Nessus Scan Information.....	52
• 24260 (1) - HyperText Transfer Protocol (HTTP) Information.....	54
• 39520 (1) - Backported Security Patch Detection (SSH).....	56
• 40665 (1) - Protected Web Page Detection.....	57
• 42085 (1) - IMAP Service STARTTLS Command Support.....	58
• 42087 (1) - POP3 Service STLS Command Support.....	59
• 42088 (1) - SMTP Service STARTTLS Command Support.....	60
• 42149 (1) - FTP Service AUTH TLS Command Support.....	61
• 43111 (1) - HTTP Methods Allowed (per directory).....	62
• 45590 (1) - Common Platform Enumeration (CPE).....	64
• 51080 (1) - Web Server Uses Basic Authentication over HTTPS.....	65
• 54580 (1) - SMTP Authentication Methods.....	66
• 54615 (1) - Device Type.....	67
• 70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported.....	68
• 70657 (1) - SSH Algorithms and Languages Supported.....	70
• 84502 (1) - HSTS Missing From HTTPS Server.....	72
• 85805 (1) - HTTP/2 Cleartext Detection.....	73
• 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided.....	74
• 117886 (1) - OS Security Patch Assessment Not Available.....	76
• 149334 (1) - SSH Password Authentication Accepted.....	77
• 153588 (1) - SSH SHA-1 HMAC Algorithms Enabled.....	78
• 181418 (1) - OpenSSH Detection.....	79

---

## **Vulnerabilities by Plugin**

---

## 54582 (1) - SMTP Service Cleartext Login Permitted

### Synopsis

The remote mail server allows cleartext logins.

### Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

### See Also

<https://tools.ietf.org/html/rfc4422>

<https://tools.ietf.org/html/rfc4954>

### Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

### Plugin Output

184.168.115.118 (tcp/587/smtp)

The SMTP server advertises the following SASL methods over an unencrypted channel on port 587 :

All supported methods : LOGIN, PLAIN  
Cleartext methods : LOGIN, PLAIN

## 70658 (1) - SSH Server CBC Mode Ciphers Enabled

### Synopsis

The SSH server is configured to use Cipher Block Chaining.

### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

### References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

### Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

### Plugin Output

184.168.115.118 (tcp/22/ssh)

The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

aes128-cbc  
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

aes128-cbc  
aes256-cbc

## 153953 (1) - SSH Weak Key Exchange Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

### Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-\*

gss-group1-sha1-\*

gss-group14-sha1-\*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### See Also

<https://datatracker.ietf.org/doc/html/rfc9142>

### Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information



## Plugin Output

---

184.168.115.118 (tcp/22/ssh)

```
The following weak key exchange algorithms are enabled :
```

```
diffie-hellman-group-exchange-sha1
```

## 11219 (13) - 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: 2024/05/20

### Plugin Output

184.168.115.118 (tcp/21)

```
Port 21/tcp was found to be open
```

184.168.115.118 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

184.168.115.118 (tcp/80/www)

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

184.168.115.118 (tcp/110/pop3)

```
Port 110/tcp was found to be open
```

184.168.115.118 (tcp/143/imap)

Port 143/tcp was found to be open

184.168.115.118 (tcp/443)

Port 443/tcp was found to be open

184.168.115.118 (tcp/587/smtp)

Port 587/tcp was found to be open

184.168.115.118 (tcp/993)

Port 993/tcp was found to be open

184.168.115.118 (tcp/2078/www)

Port 2078/tcp was found to be open

184.168.115.118 (tcp/2082)

Port 2082/tcp was found to be open

184.168.115.118 (tcp/2083)

Port 2083/tcp was found to be open

184.168.115.118 (tcp/2095)

Port 2095/tcp was found to be open

184.168.115.118 (tcp/3306/mysql)

Port 3306/tcp was found to be open

## 22964 (6) - 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

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

184.168.115.118 (tcp/80/www)

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

184.168.115.118 (tcp/110/pop3)

```
A POP3 server is running on this port.
```

184.168.115.118 (tcp/143/imap)

```
An IMAP server is running on this port.
```

184.168.115.118 (tcp/587/smtp)

```
An SMTP server is running on this port.
```

184.168.115.118 (tcp/2078/www)

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

184.168.115.118 (tcp/2078/www)

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

## 10863 (4) - 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

184.168.115.118 (tcp/21)

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 64 DB 1B 5E 93 3A AE F8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 16 18:09:08 2024 GMT
Not Valid After: Mar 19 18:09:08 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D8 D0 0D 21 F0 EC 30 95 AD E0 46 C8 34 93 D8 98 0E D8 C8
            A3 8F DF 13 5D 8D 7F C9 13 46 C8 03 0F CB 87 EA 01 37 5E CE
            62 BD E6 C4 D8 B3 5D 4E D1 D5 A6 98 C0 D6 75 CA C3 53 4E AF
            AF 3A AE 21 12 0D 65 F2 F4 7B BE 30 6C 6C 1A 14 95 75 DB 09
            99 50 FD A8 E3 76 33 61 26 1D 07 89 4A 58 97 60 8C 7D 83 8D
```

```
58 F4 2E A6 2F 3C C3 04 27 30 68 B8 2B 08 F1 18 CC 5B 0B 79
1E DA 98 ED 6B DF 24 39 8A 6B A8 52 52 03 4B 61 54 9C 5F 80
33 7F 99 3D 4D B4 25 98 7C 9A CF 5B CF 03 3A 68 8E 69 72 02
0B BA 07 D6 34 D5 07 1F EB 9F 47 8C A0 55 D1 68 59 54 58 EA
45 E0 41 23 15 BE D0 76 CE 2C 36 F7 24 BA EA 1F 45 B7 9B A9
9C D6 B0 67 80 75 3F 3B 4C 93 2F 54 4A 22 81 24 E9 33 8F 2A
4B B9 10 39 DF D6 54 99 DF CF 66 A7 36 42 30 65 09 D4 54 F2
7F 41 1F 98 D8 02 67 0F 5F 7D CD 2F 8F 77 B9 19 1D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 2C 3D FE BA 42 8D 4D 2C D1 0A F2 C5 8F CA D5 B8 12 CE F8
C3 91 99 3C 35 44 7D FE 4C 0D 10 FB 2A 95 75 CC 3E B2 68 AF
D6 F1 1F 0A 1A ED C0 E1 67 1D 74 5A B0 3D CA C2 E3 6A 80 21
FD 39 B2 2E 8E F4 0B D7 58 53 E8 09 EE 03 69 8B 01 7B 7E F3
DB AC A4 1E 55 26 89 4E C8 C3 7E 6E 4E 11 55 C9 23 76 F3 31
F7 51 79 52 2C B1 86 14 DA 07 10 6D C4 C9 A5 4A 60 13 61 07
CF D8 95 42 ED 4E E7 F0 31 92 61 27 8C 27 ED 6D 88 BC D [...]
```

184.168.115.118 (tcp/110/pop3)

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 64 DB 1B 5E 93 3A AE F8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 16 18:09:08 2024 GMT
Not Valid After: Mar 19 18:09:08 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D8 D0 0D 21 F0 EC 30 95 AD E0 46 C8 34 93 D8 98 0E D8 C8
A3 8F DF 13 5D 8D 7F C9 13 46 C8 03 0F CB 87 EA 01 37 5E CE
62 BD E6 C4 D8 B3 5D 4E D1 D5 A6 98 C0 D6 75 CA C3 53 4E AF
AF 3A AE 21 12 0D 65 F2 F4 7B BE 30 6C 6C 1A 14 95 75 DB 09
99 50 FD A8 E3 76 33 61 26 1D 07 89 4A 58 97 60 8C 7D 83 8D
58 F4 2E A6 2F 3C C3 04 27 30 68 B8 2B 08 F1 18 CC 5B 0B 79
1E DA 98 ED 6B DF 24 39 8A 6B A8 52 52 03 4B 61 54 9C 5F 80
33 7F 99 3D 4D B4 25 98 7C 9A CF 5B CF 03 3A 68 8E 69 72 02
0B BA 07 D6 34 D5 07 1F EB 9F 47 8C A0 55 D1 68 59 54 58 EA
45 E0 41 23 15 BE D0 76 CE 2C 36 F7 24 BA EA 1F 45 B7 9B A9
9C D6 B0 67 80 75 3F 3B 4C 93 2F 54 4A 22 81 24 E9 33 8F 2A
4B B9 10 39 DF D6 54 99 DF CF 66 A7 36 42 30 65 09 D4 54 F2
7F 41 1F 98 D8 02 67 0F 5F 7D CD 2F 8F 77 B9 19 1D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 2C 3D FE BA 42 8D 4D 2C D1 0A F2 C5 8F CA D5 B8 12 CE F8
C3 91 99 3C 35 44 7D FE 4C 0D 10 FB 2A 95 75 CC 3E B2 68 AF
D6 F1 1F 0A 1A ED C0 E1 67 1D 74 5A B0 3D CA C2 E3 6A 80 21
FD 39 B2 2E 8E F4 0B D7 58 53 E8 09 EE 03 69 8B 01 7B 7E F3
DB AC A4 1E 55 26 89 4E C8 C3 7E 6E 4E 11 55 C9 23 76 F3 31
```

```
F7 51 79 52 2C B1 86 14 DA 07 10 6D C4 C9 A5 4A 60 13 61 07
CF D8 95 42 ED 4E E7 F0 31 92 61 27 8C 27 ED 6D 88 BC D [...]
```

## 184.168.115.118 (tcp/143/imap)

Subject Name:

Common Name: \*.prod.sin2.secureserver.net

Issuer Name:

Country: US

State/Province: Arizona

Locality: Scottsdale

Organization: Starfield Technologies, Inc.

Organization Unit: <http://certs.starfieldtech.com/repository/>

Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 64 DB 1B 5E 93 3A AE F8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 16 18:09:08 2024 GMT

Not Valid After: Mar 19 18:09:08 2025 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 D8 D0 0D 21 F0 EC 30 95 AD E0 46 C8 34 93 D8 98 0E D8 C8  
A3 8F DF 13 5D 8D 7F C9 13 46 C8 03 0F CB 87 EA 01 37 5E CE  
62 BD E6 C4 D8 B3 5D 4E D1 D5 A6 98 C0 D6 75 CA C3 53 4E AF  
AF 3A AE 21 12 0D 65 F2 F4 7B BE 30 6C 6C 1A 14 95 75 DB 09  
99 50 FD A8 E3 76 33 61 26 1D 07 89 4A 58 97 60 8C 7D 83 8D  
58 F4 2E A6 2F 3C C3 04 27 30 68 B8 2B 08 F1 18 CC 5B 0B 79  
1E DA 98 ED 6B DF 24 39 8A 6B A8 52 52 03 4B 61 54 9C 5F 80  
33 7F 99 3D 4D B4 25 98 7C 9A CF 5B CF 03 3A 68 8E 69 72 02  
0B BA 07 D6 34 D5 07 1F EB 9F 47 8C A0 55 D1 68 59 54 58 EA  
45 E0 41 23 15 BE D0 76 CE 2C 36 F7 24 BA EA 1F 45 B7 9B A9  
9C D6 B0 67 80 75 3F 3B 4C 93 2F 54 4A 22 81 24 E9 33 8F 2A  
4B B9 10 39 DF D6 54 99 DF CF 66 A7 36 42 30 65 09 D4 54 F2  
7F 41 1F 98 D8 02 67 0F 5F 7D CD 2F 8F 77 B9 19 1D

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 2C 3D FE BA 42 8D 4D 2C D1 0A F2 C5 8F CA D5 B8 12 CE F8  
C3 91 99 3C 35 44 7D FE 4C 0D 10 FB 2A 95 75 CC 3E B2 68 AF  
D6 F1 1F 0A 1A ED C0 E1 67 1D 74 5A B0 3D CA C2 E3 6A 80 21  
FD 39 B2 2E 8E F4 0B D7 58 53 E8 09 EE 03 69 8B 01 7B 7E F3  
DB AC A4 1E 55 26 89 4E C8 C3 7E 6E 4E 11 55 C9 23 76 F3 31  
F7 51 79 52 2C B1 86 14 DA 07 10 6D C4 C9 A5 4A 60 13 61 07  
CF D8 95 42 ED 4E E7 F0 31 92 61 27 8C 27 ED 6D 88 BC D [...]

## 184.168.115.118 (tcp/2078/www)

Subject Name:

Common Name: \*.prod.sin2.secureserver.net

Issuer Name:

Country: US

State/Province: Arizona



Locality: Scottsdale  
Organization: Starfield Technologies, Inc.  
Organization Unit: <http://certs.starfieldtech.com/repository/>  
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 64 DB 1B 5E 93 3A AE F8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 16 18:09:08 2024 GMT  
Not Valid After: Mar 19 18:09:08 2025 GMT

Public Key Info:

Algorithm: RSA Encryption  
Key Length: 2048 bits  
Public Key: 00 D8 D0 0D 21 F0 EC 30 95 AD E0 46 C8 34 93 D8 98 0E D8 C8  
A3 8F DF 13 5D 8D 7F C9 13 46 C8 03 0F CB 87 EA 01 37 5E CE  
62 BD E6 C4 D8 B3 5D 4E D1 D5 A6 98 C0 D6 75 CA C3 53 4E AF  
AF 3A AE 21 12 0D 65 F2 F4 7B BE 30 6C 6C 1A 14 95 75 DB 09  
99 50 FD A8 E3 76 33 61 26 1D 07 89 4A 58 97 60 8C 7D 83 8D  
58 F4 2E A6 2F 3C C3 04 27 30 68 B8 2B 08 F1 18 CC 5B 0B 79  
1E DA 98 ED 6B DF 24 39 8A 6B A8 52 52 03 4B 61 54 9C 5F 80  
33 7F 99 3D 4D B4 25 98 7C 9A CF 5B CF 03 3A 68 8E 69 72 02  
0B BA 07 D6 34 D5 07 1F EB 9F 47 8C A0 55 D1 68 59 54 58 EA  
45 E0 41 23 15 BE D0 76 CE 2C 36 F7 24 BA EA 1F 45 B7 9B A9  
9C D6 B0 67 80 75 3F 3B 4C 93 2F 54 4A 22 81 24 E9 33 8F 2A  
4B B9 10 39 DF D6 54 99 DF CF 66 A7 36 42 30 65 09 D4 54 F2  
7F 41 1F 98 D8 02 67 0F 5F 7D CD 2F 8F 77 B9 19 1D

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits  
Signature: 00 2C 3D FE BA 42 8D 4D 2C D1 0A F2 C5 8F CA D5 B8 12 CE F8  
C3 91 99 3C 35 44 7D FE 4C 0D 10 FB 2A 95 75 CC 3E B2 68 AF  
D6 F1 1F 0A 1A ED C0 E1 67 1D 74 5A B0 3D CA C2 E3 6A 80 21  
FD 39 B2 2E 8E F4 0B D7 58 53 E8 09 EE 03 69 8B 01 7B 7E F3  
DB AC A4 1E 55 26 89 4E C8 C3 7E 6E 4E 11 55 C9 23 76 F3 31  
F7 51 79 52 2C B1 86 14 DA 07 10 6D C4 C9 A5 4A 60 13 61 07  
CF D8 95 42 ED 4E E7 F0 31 92 61 27 8C 27 ED 6D 88 BC D [...]

## 21643 (4) - 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: 2023/07/10

### Plugin Output

184.168.115.118 (tcp/21)

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_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					
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-AES-128-CCM8-AEAD AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(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-AES-256-CCM8-AEAD AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(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	0xC0, 0x76	ECDH	RSA	[...]

184.168.115.118 (tcp/110/pop3)

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_CCM_SHA256 AEAD	0x13, 0x04	-	-	AES-CCM(128)	
TLS_AES_128_GCM_SHA256 AEAD	0x13, 0x01	-	-	AES-GCM(128)	
TLS_AES_256_GCM_SHA384 AEAD	0x13, 0x02	-	-	AES-GCM(256)	
TLS_CHACHA20_POLY1305_SHA256 AEAD	0x13, 0x03	-	-	ChaCha20-Poly1305(256)	

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
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-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	

The fields above are :

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

Note that this service does not encrypt traffic by default but does support upgrading to an encrypted connection using STARTTLS.

## 184.168.115.118 (tcp/143/imap)

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_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					
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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
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	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	
SHA256					

The fields above are :

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

Note that this service does not encrypt traffic by default but does support upgrading to an encrypted connection using STARTTLS.

## 184.168.115.118 (tcp/2078/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_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)
AEAD				
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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
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	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	
SHA256					

The fields above are :

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

## 45410 (4) - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

184.168.115.118 (tcp/21)

```
The host name known by Nessus is :  
    118.115.168.184.host.secureserver.net  
  
The Common Name in the certificate is :  
    *.prod.sin2.secureserver.net  
  
The Subject Alternate Names in the certificate are :  
    *.prod.sin2.secureserver.net  
    prod.sin2.secureserver.net
```

184.168.115.118 (tcp/110/pop3)

```
The host name known by Nessus is :  
    118.115.168.184.host.secureserver.net  
  
The Common Name in the certificate is :  
    *.prod.sin2.secureserver.net  
  
The Subject Alternate Names in the certificate are :
```

```
*.prod.sin2.secureserver.net  
prod.sin2.secureserver.net
```

### 184.168.115.118 (tcp/143/imap)

The host name known by Nessus is :

```
118.115.168.184.host.secureserver.net
```

The Common Name in the certificate is :

```
*.prod.sin2.secureserver.net
```

The Subject Alternate Names in the certificate are :

```
*.prod.sin2.secureserver.net  
prod.sin2.secureserver.net
```

### 184.168.115.118 (tcp/2078/www)

The host name known by Nessus is :

```
118.115.168.184.host.secureserver.net
```

The Common Name in the certificate is :

```
*.prod.sin2.secureserver.net
```

The Subject Alternate Names in the certificate are :

```
*.prod.sin2.secureserver.net  
prod.sin2.secureserver.net
```

## 56984 (4) - 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

184.168.115.118 (tcp/21)

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

184.168.115.118 (tcp/110/pop3)

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

184.168.115.118 (tcp/143/imap)

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

184.168.115.118 (tcp/2078/www)

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



## 57041 (4) - 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

184.168.115.118 (tcp/21)

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-AES-128-CCM8-AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(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-AES-256-CCM8-AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)	
AEAD					

DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(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)
ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(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	0xC0, 0x13	ECDH	RSA	AES-CBC(128) [...]

## 184.168.115.118 (tcp/110/pop3)

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-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
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-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	

The fields above are :

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

## 184.168.115.118 (tcp/143/imap)

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-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	

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	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
SHA384				
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
SHA256				

The fields above are :

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

184.168.115.118 (tcp/2078/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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
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	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	
SHA256					

The fields above are :

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

## 94761 (4) - 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\(v=ws.10\)](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

### Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

### Plugin Output

184.168.115.118 (tcp/21)

The following root Certification Authority certificate was found :

```
| -Subject          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Issuer          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Valid From      : Jun 29 17:39:16 2004 GMT
| -Valid To       : Jun 29 17:39:16 2034 GMT
| -Signature Algorithm : SHA-1 With RSA Encryption
```

184.168.115.118 (tcp/110/pop3)

The following root Certification Authority certificate was found :

```
| -Subject          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
```

```
| -Issuer          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Valid From      : Jun 29 17:39:16 2004 GMT
| -Valid To        : Jun 29 17:39:16 2034 GMT
| -Signature Algorithm : SHA-1 With RSA Encryption
```

#### 184.168.115.118 (tcp/143/imap)

The following root Certification Authority certificate was found :

```
| -Subject          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Issuer          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Valid From      : Jun 29 17:39:16 2004 GMT
| -Valid To        : Jun 29 17:39:16 2034 GMT
| -Signature Algorithm : SHA-1 With RSA Encryption
```

#### 184.168.115.118 (tcp/2078/www)

The following root Certification Authority certificate was found :

```
| -Subject          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Issuer          : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
| Authority
| -Valid From      : Jun 29 17:39:16 2004 GMT
| -Valid To        : Jun 29 17:39:16 2034 GMT
| -Signature Algorithm : SHA-1 With RSA Encryption
```

## 95631 (4) - 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	11849
BID	33065
XREF	CWE:310

### Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

## Plugin Output

### 184.168.115.118 (tcp/21)

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=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : Jun 29 17:39:16 2004 GMT
Valid To        : Jun 29 17:39:16 2034 GMT
```

Raw PEM certificate :

-----BEGIN CERTIFICATE-----

```
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjEw
+6XGmBIWtDBFk385N78gDGIC/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDir1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azb15KXznJHoeOnRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCBM0GA1UdDgQWBBS/X7fRzt0fhvRbVazclxDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazclxDCDqmI56FspGowaDELMakGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPuXA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvvggQQt08PT7dL5WXXp59fkdhEmt1b71cZBDzI0fmgAKhympVSJYACPq4xJDKVtHCN2MQWp1Bq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

### 184.168.115.118 (tcp/110/pop3)

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=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : Jun 29 17:39:16 2004 GMT
Valid To        : Jun 29 17:39:16 2034 GMT
```

Raw PEM certificate :

-----BEGIN CERTIFICATE-----

```
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjEw
+6XGmBIWtDBFk385N78gDGIC/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDir1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azb15KXznJHoeOnRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCBM0GA1UdDgQWBBS/X7fRzt0fhvRbVazclxDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazclxDCDqmI56FspGowaDELMakGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPuXA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvvggQQt08PT7dL5WXXp59fkdhEmt1b71cZBDzI0fmgAKhympVSJYACPq4xJDKVtHCN2MQWp1Bq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

### 184.168.115.118 (tcp/143/imap)

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=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : Jun 29 17:39:16 2004 GMT
Valid To         : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEZzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ211cywgSW5jLjE/
+6XGmBIWtDBFk385N78gDGIC/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDir1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBWj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azb15KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPuXa2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvqgQQto8PT7dL5WXXp59fkdhEmt1b71cZBDzI0fmqAKhympVSJYACPq4xJDKVtHCN2MQWp1BQ
D5fs4C8fF5Q=
-----END CERTIFICATE-----

```

184.168.115.118 (tcp/2078/www)

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=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : Jun 29 17:39:16 2004 GMT
Valid To         : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEZzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ211cywgSW5jLjE/
+6XGmBIWtDBFk385N78gDGIC/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDir1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBWj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azb15KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPuXa2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvqgQQto8PT7dL5WXXp59fkdhEmt1b71cZBDzI0fmqAKhympVSJYACPq4xJDKVtHCN2MQWp1BQ
D5fs4C8fF5Q=
-----END CERTIFICATE-----

```



## 136318 (4) - 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

### Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

### Plugin Output

184.168.115.118 (tcp/21)

```
TLShv1.2 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/110/pop3)

```
TLShv1.2 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/143/imap)

```
TLShv1.2 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/2078/www)

```
TLShv1.2 is enabled and the server supports at least one cipher.
```

## 138330 (4) - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

<https://tools.ietf.org/html/rfc8446>

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

### Plugin Output

184.168.115.118 (tcp/21)

```
TLShv1.3 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/110/pop3)

```
TLShv1.3 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/143/imap)

```
TLShv1.3 is enabled and the server supports at least one cipher.
```

184.168.115.118 (tcp/2078/www)

```
TLShv1.3 is enabled and the server supports at least one cipher.
```

## 156899 (4) - 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

## 184.168.115.118 (tcp/21)

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-AES-128-CCM8-AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(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-AES-256-CCM8-AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(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-AES-128-CCM8-AEAD	0xC0, 0xA0	RSA	RSA	AES-CCM8(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-AES-256-CCM8-AEAD	0xC0, 0xA1	RSA	RSA	AES-CCM8(256)	
AEAD					
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
SHA384					
TLS_AES_128_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH [...]			

## 184.168.115.118 (tcp/110/pop3)

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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
TLS_AES_128_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
```

```
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

## 184.168.115.118 (tcp/143/imap)

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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
TLS_AES_128_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					

The fields above are :

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

## 184.168.115.118 (tcp/2078/www)

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-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
TLS_AES_128_CCM_SHA256	0x13, 0x04	-	-	AES-CCM(128)	
AEAD					

The fields above are :

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

## 10092 (1) - FTP Server Detection

### Synopsis

An FTP server is listening on a remote port.

### Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0943

### Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

### Plugin Output

184.168.115.118 (tcp/21)

The remote FTP banner is :

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 02:46. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

## 10107 (1) - 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

184.168.115.118 (tcp/2078/www)

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

```
cPanel
```

## 10185 (1) - POP Server Detection

### Synopsis

A POP server is listening on the remote port.

### Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

### See Also

[https://en.wikipedia.org/wiki/Post\\_Office\\_Protocol](https://en.wikipedia.org/wiki/Post_Office_Protocol)

### Solution

Disable this service if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

### Plugin Output

184.168.115.118 (tcp/110/pop3)

```
Remote POP server banner :
```

```
+OK Dovecot ready.
```



## 10263 (1) - SMTP Server Detection

### Synopsis

An SMTP server is listening on the remote port.

### Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

### Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

### Risk Factor

None

### References

XREF IAVT:0001-T-0932

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

184.168.115.118 (tcp/587/smtp)

Remote SMTP server banner :

```
220-sg2plzcpnl490071.prod.sin2.secureserver.net ESMTP Exim 4.96.2 #2 Mon, 01 Jul 2024 02:41:17
-0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

## 10267 (1) - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0933

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

184.168.115.118 (tcp/22/ssh)

```
SSH version : SSH-2.0-OpenSSH_8.0
SSH supported authentication : publickey,password
```

## 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

184.168.115.118 (udp/0)

```
For your information, here is the traceroute from 192.168.157.129 to 184.168.115.118 :  
192.168.157.129  
192.168.157.2  
184.168.115.118
```

```
Hop Count: 2
```

## 10719 (1) - MySQL Server Detection

### Synopsis

A database server is listening on the remote port.

### Description

The remote host is running MySQL, an open source database server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0802

### Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

### Plugin Output

184.168.115.118 (tcp/3306/mysql)

```
Version : 5.5.5-10.6.18-MariaDB-cll-lve
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

## 10881 (1) - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

### Plugin Output

184.168.115.118 (tcp/22/ssh)

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

## 11153 (1) - Service Detection (HELP Request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

### Plugin Output

184.168.115.118 (tcp/3306/mysql)

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

## 11414 (1) - IMAP Service Banner Retrieval

### Synopsis

An IMAP server is running on the remote host.

### Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

### Plugin Output

184.168.115.118 (tcp/143/imap)

The remote imap server banner is :

```
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS  
AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

## 11424 (1) - WebDAV Detection

### Synopsis

The remote server is running with WebDAV enabled.

### Description

WebDAV is an industry standard extension to the HTTP specification.

It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

### Solution

<http://support.microsoft.com/default.aspx?kbid=241520>

### Risk Factor

None

### Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

### Plugin Output

184.168.115.118 (tcp/2078/www)



## 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: 2024/06/19

### Plugin Output

184.168.115.118 (tcp/0)

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP
```

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](mailto: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.

```
SSH:!:SSH-2.0-OpenSSH_8.0
```

```
SinFP:
```

```
P1:B11013:F0x12:W64240:00204ffff:M1460:
```

```
P2:B11013:F0x12:W64240:00204ffff:M1460:
```

```
P3:B00000:F0x00:W0:00:M0
```

```
P4:190804_7_p=443R
```

```
HTTP:!:Server: Apache
```

```
SMTP:!:220-sg2plzcpnl490071.prod.sin2.secureserver.net ESMTP Exim 4.96.2 #2 Mon, 01 Jul 2024
02:41:17 -0700
```

```
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

```
SSLcert:!:i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/
OU:http://certs.starfieldtech.com/repository/s/CN:*.prod.sin2.secureserver.net
2ac95f2eb27bb3b3b90a417b5747d6fc2a665462
```

```
i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/OU:http://
certs.starfieldtech.com/repository/s/CN:*.prod.sin2.secureserver.net
```

2ac95f2eb27bb3b3b90a417b5747d6fc2a665462

The remote host is running CISCO PIX 7.0

## 12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

### Synopsis

It was possible to resolve the name of the remote host.

### Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

### Plugin Output

184.168.115.118 (tcp/0)

```
184.168.115.118 resolves as 118.115.168.184.host.secureserver.net.
```

## 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: 2024/06/04

### Plugin Output

184.168.115.118 (tcp/0)

Information about this scan :

```
Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406302007
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
```

```
Scan name : cogent company
Scan policy used : Basic Network Scan
Scanner IP : 192.168.157.129
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 50.071 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 : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/7/1 4:01 EDT
Scan duration : 7316 sec
Scan for malware : no
```

## 24260 (1) - 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

184.168.115.118 (tcp/2078/www)

Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : yes

Keep-Alive : no

Options allowed : POST, UNLOCK, PROPFIND, OPTIONS, COPY, DELETE, PROPPATCH, LOCK, MKCOL, PUT, HEAD, MOVE, GET

Headers :

Date: Mon, 01 Jul 2024 09:57:14 GMT

Server: cPanel

Persistent-Auth: false

Host: 118.115.168.184.host.secureserver.net:2078

Cache-Control: no-cache, no-store, must-revalidate, private

Connection: close

Vary: Accept-Encoding

WWW-Authenticate: Basic realm="Restricted Area"

Content-Length: 35

Content-Type: text/html; charset="utf-8"

Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

```
<html>Authorization Required</html>
```

## 39520 (1) - Backported Security Patch Detection (SSH)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

[https://access.redhat.com/security/updates/backporting/?sc\\_cid=3093](https://access.redhat.com/security/updates/backporting/?sc_cid=3093)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

184.168.115.118 (tcp/22/ssh)

Give Nessus credentials to perform local checks.



## 40665 (1) - Protected Web Page Detection

### Synopsis

Some web pages require authentication.

### Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.
- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

### Plugin Output

184.168.115.118 (tcp/2078/www)

The following pages are protected by the Basic authentication scheme :

/

## 42085 (1) - IMAP Service STARTTLS Command Support

### Synopsis

The remote mail service supports encrypting traffic.

### Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc2595>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

### Plugin Output

184.168.115.118 (tcp/143/imap)

The remote IMAP service responded to the 'STARTTLS' command with an 'OK' response code, suggesting that it supports that command. However, Nessus failed to negotiate a TLS connection or get the associated SSL certificate, perhaps because of a network connectivity problem or the service requires a peer certificate as part of the negotiation.

## 42087 (1) - POP3 Service STLS Command Support

### Synopsis

The remote mail service supports encrypting traffic.

### Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc2595>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

### Plugin Output

184.168.115.118 (tcp/110/pop3)

```
The remote POP3 service responded to the 'STLS' command with an
'+OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

## 42088 (1) - SMTP Service STARTTLS Command Support

### Synopsis

The remote mail service supports encrypting traffic.

### Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc2487>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

### Plugin Output

184.168.115.118 (tcp/587/smtp)

The remote SMTP service responded to the 'STARTTLS' command with a '220' response code, suggesting that it supports that command. However, Nessus failed to negotiate a TLS connection or get the associated SSL certificate, perhaps because of a network connectivity problem or the service requires a peer certificate as part of the negotiation.

## 42149 (1) - FTP Service AUTH TLS Command Support

### Synopsis

The remote directory service supports encrypting traffic.

### Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc4217>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/15, Modified: 2024/01/16

### Plugin Output

184.168.115.118 (tcp/21)

The remote FTP service responded to the 'AUTH TLS' command with a '234' response code, suggesting that it supports that command. However, Nessus failed to negotiate a TLS connection or get the associated SSL certificate, perhaps because of a network connectivity problem or the service requires a peer certificate as part of the negotiation.

## 43111 (1) - 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\\_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

184.168.115.118 (tcp/2078/www)

Based on the response to an OPTIONS request :

- HTTP methods COPY DELETE GET HEAD LOCK MKCOL OPTIONS POST  
PROPFIND PROPPATCH PUT UNLOCK MOVE are allowed on :

/

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND  
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD  
INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY  
OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT  
RPC\_IN\_DATA RPC\_OUT\_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK  
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

## 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: 2024/06/24

### Plugin Output

184.168.115.118 (tcp/0)

The remote operating system matched the following CPE :

cpe:/o:cisco:pix\_firewall:7.0 -> Cisco PIX Firewall Software

Following application CPE's matched on the remote system :

cpe:/a:mariadb:mariadb:10.6.18 -> MariaDB for Node.js

cpe:/a:mysql:mysql:5.5.5-10.6.18-mariadb-cll-lve -> MySQL MySQL

cpe:/a:openbsd:openssh:8.0 -> OpenBSD OpenSSH



## 51080 (1) - Web Server Uses Basic Authentication over HTTPS

### Synopsis

The remote web server seems to transmit credentials using Basic Authentication.

### Description

The remote web server contains web pages that are protected by 'Basic' authentication over HTTPS.

While this is not in itself a security flaw, in some organizations, the use of 'Basic' authentication is discouraged as, depending on the underlying implementation, it may be vulnerable to account brute-forcing or may encourage Man-in-The-Middle (MiTM) attacks.

### Solution

Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.

### Risk Factor

None

### Plugin Information

Published: 2010/12/08, Modified: 2011/03/18

### Plugin Output

184.168.115.118 (tcp/2078/www)

```
The following pages are protected :
```

```
/:/ realm="Restricted Area"
```

## 54580 (1) - SMTP Authentication Methods

### Synopsis

The remote mail server supports authentication.

### Description

The remote SMTP server advertises that it supports authentication.

### See Also

<https://tools.ietf.org/html/rfc4422>

<https://tools.ietf.org/html/rfc4954>

### Solution

Review the list of methods and whether they're available over an encrypted channel.

### Risk Factor

None

### Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

### Plugin Output

184.168.115.118 (tcp/587/smtp)

The following authentication methods are advertised by the SMTP server without encryption :

LOGIN

PLAIN

## 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: 2022/09/09

### Plugin Output

184.168.115.118 (tcp/0)

```
Remote device type : firewall  
Confidence level : 70
```

## 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

184.168.115.118 (tcp/21)

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)	[...]

## 70657 (1) - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

### Plugin Output

184.168.115.118 (tcp/22/ssh)

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for `kex_algorithms` :

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
kex-strict-s-v00@openssh.com
```

The server supports the following options for `server_host_key_algorithms` :

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-256-cert-v01@openssh.com
rsa-sha2-512
rsa-sha2-512-cert-v01@openssh.com
ssh-ed25519
ssh-rsa
ssh-rsa-cert-v01@openssh.com
```

The server supports the following options for `encryption_algorithms_client_to_server` :

```
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
zlib@openssh.com
```

The server supports the following options for `compression_algorithms_server_to_client` :

```
none
zlib@openssh.com
```

## 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: 2021/05/19

### Plugin Output

184.168.115.118 (tcp/2078/www)

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



## 85805 (1) - HTTP/2 Cleartext Detection

### Synopsis

An HTTP/2 server is listening on the remote host.

### Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

### See Also

<https://http2.github.io/>

<https://tools.ietf.org/html/rfc7540>

<https://github.com/http2/http2-spec>

### Solution

Limit incoming traffic to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

### Plugin Output

184.168.115.118 (tcp/80/www)

```
The server supports direct HTTP/2 connections
without encryption.
```

## 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

### Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVB:0001-B-0504

### Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

### Plugin Output

184.168.115.118 (tcp/0)

SSH was detected on port 22 but no credentials were provided.

SSH local checks were not enabled.

## 117886 (1) - OS Security Patch Assessment Not Available

### Synopsis

OS Security Patch Assessment is not available.

### Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVB:0001-B-0515

### Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

### Plugin Output

184.168.115.118 (tcp/0)

The following issues were reported :

```
- Plugin      : no_local_checks_credentials.nasl
  Plugin ID   : 110723
  Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
  Message     :
  Credentials were not provided for detected SSH service.
```

## 149334 (1) - SSH Password Authentication Accepted

### Synopsis

The SSH server on the remote host accepts password authentication.

### Description

The SSH server on the remote host accepts password authentication.

### See Also

<https://tools.ietf.org/html/rfc4252#section-8>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

### Plugin Output

184.168.115.118 (tcp/22/ssh)

## 153588 (1) - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

### Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

### Plugin Output

184.168.115.118 (tcp/22/ssh)

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1
hmac-sha1-etm@openssh.com
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1
hmac-sha1-etm@openssh.com
```

## 181418 (1) - OpenSSH Detection

### Synopsis

An OpenSSH-based SSH server was detected on the remote host.

### Description

An OpenSSH-based SSH server was detected on the remote host.

### See Also

<https://www.openssh.com/>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/09/14, Modified: 2024/06/28

### Plugin Output

184.168.115.118 (tcp/22/ssh)

```
Service : ssh
Version : 8.0
Banner  : SSH-2.0-OpenSSH_8.0
```