MOMENTUM

THREADSCAN

Example Report

RESULTS

TOTAL OVERVIEW OF OPEN VULNERABILITIES BY: 03-07-2024

CRITICAL	HIGH	MEDIUM	LOW
3	4	16	7

OPEN VULNERABILITIES BY: 03-07-2024

Classification	Short description	Action	Count	Info
CRITICAL	The remote service encrypts traffic using a protocol with known weaknesses.	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	3	
CRITICAL	The operating system running on the remote host is no longer supported.	Upgrade to a version of the Unix operating system that is currently supported.	1	
CRITICAL	The remote device is missing a vendor-supplied security patch.	Upgrade to the relevant fixed version referenced in Cisco Security Advisories cisco-sa-20160210-asa-ike and cisco-sa-20160323-ios-ikev2.	1	
HIGH	The remote service supports the use of medium strength SSL ciphers.	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	9	
HIGH	The remote mail server is affected by an information disclosure vulnerability.	Only attack two (Reverse Proxy / Gateway) is fixed in current versions. Apply the latest supplied vendor patches.	1	
HIGH	The remote Apache Tomcat server is affected by multiple vulnerabilities.	Update to Apache Tomcat version 6.0.43 or later.	1	

Classification	Short description	Action	Count	Info
HIGH	The remote web server hosts a PHP application that is affected by a SQL injection vulnerability.	Upgrade to phpMyAdmin version 4.9.4, 5.0.1, or later. Alternatively, apply the patches referenced in the vendor advisories.	1	
MEDIUM	The remote web server is not enforcing HSTS, as defined by RFC 6797.	Configure the remote web server to use HSTS.	5	
MEDIUM	The SSL certificate for this service cannot be trusted.	Purchase or generate a proper SSL certificate for this service.	9	
MEDIUM	The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	Purchase or generate a proper SSL certificate for this service.	5	
MEDIUM	The remote service supports the use of the RC4 cipher.	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	6	
MEDIUM	The remote service encrypts traffic using an older version of TLS.	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	12	
MEDIUM	The remote service encrypts traffic using an older version of TLS.	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	12	
MEDIUM	It is possible to retrieve file backups from the remote web server.	Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.	1	
MEDIUM	The remote web server contains default files.	Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.	1	
MEDIUM	The remote server's SSL certificate has already expired.	Purchase or generate a new SSL certificate to replace the existing one.	3	

Classification	Short description	Action	Count	Info
MEDIUM	The remote web server discloses process information.	Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.	1	
MEDIUM	The remote SMTP service is running on a non-standard port.	Check and clean the configuration.	1	
MEDIUM	Some directories on the remote web server are browsable.	Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.	2	
MEDIUM	The SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.	1	
MEDIUM	The remote IKEv1 service supports Aggressive Mode with Pre-Shared key.	- Disable Aggressive Mode if supported. - Do not use Pre-Shared key for authentication if it's possible. - If using Pre-Shared key cannot be avoided, use very strong keys. - If possible, do not allow VPN connections from any IP addresses. Note that this plugin does not run over IPv6.	1	
MEDIUM	The remote web server may fail to mitigate a class of web application vulnerabilities.	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.	3	
MEDIUM	The remote NTP server responds to mode 6 queries.	Restrict NTP mode 6 queries.	1	
LOW	It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.	3	

Classification	Short description	Action	Count	Info
LOW	It is possible to determine the exact time set on the remote host.	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).	2	
LOW	This web server leaks a private IP address through its HTTP headers.	Apply configuration suggested by vendor.	2	
LOW	The remote web server might transmit credentials in cleartext.	Make sure that every sensitive form transmits content over HTTPS.	1	
LOW	The 'autocomplete' attribute is not disabled on password fields.	Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.	3	
LOW	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.	3	
LOW	The remote SSH server is configured to allow weak key exchange algorithms.	Contact the vendor or consult product documentation to disable the weak algorithms.	1	

DETAILED INFORMATION

SSL Version 2 and 3 Protocol Detection

Plugin ID	**20007**
Family	**Service detection**
Exploit Available	**false**
Severity	**CRITICAL**

ThreadStone explanation:

The external service encrypts traffic using a protocol with known weaknesses. This can lead to the following risks:

1. Eavesdropping: Malicious actors can intercept the traffic and potentially crack the weak encryption, giving them access to sensitive information.
2. Data leaks: If the encryption is breached, personal data or trade secrets can be leaked.
3. Man-in-the-Middle attacks (MitM): Attackers can position themselves between the server and the client, manipulating or redirecting the communication.

It is important for the service to switch to a stronger encryption method to mitigate these risks.

Synopsis:

The remote service encrypts traffic using a protocol with known weaknesses.

Solution:

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Host:

000.000.193.139, 000.000.193.53, 000.000.193.54

See also:

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Plugin output:

```
Ports: 000.000.193.53:444

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                          Code            KEX          Auth     Encryption            MAC
-----------------------       ----------      ---          ----     ---------------------  ---
DES-CBC3-SHA                                  RSA          RSA      3DES-CBC(168)         SHA1

High Strength Ciphers (>= 112-bit key)

Name                          Code            KEX          Auth     Encryption            MAC
```

```
----------------------        ----------       ---          ----     --------------------  ---
DHE-RSA-AES128-SHA                             DH           RSA      AES-CBC(128)          SHA1
DHE-RSA-AES256-SHA                             DH           RSA      AES-CBC(256)          SHA1
ECDHE-RSA-AES128-SHA                           ECDH         RSA      AES-CBC(128)          SHA1
ECDHE-RSA-AES256-SHA                           ECDH         RSA      AES-CBC(256)          SHA1
AES128-SHA                                     RSA          RSA      AES-CBC(128)          SHA1
AES256-SHA                                     RSA          RSA      AES-CBC(256)          SHA1
RC4-MD5                                        RSA          RSA      RC4(128)              MD5
RC4-SHA                                        RSA          RSA      RC4(128)              SHA1
ECDHE-RSA-AES128-SHA256                        ECDH         RSA      AES-CBC(128)          SHA256
ECDHE-RSA-AES256-SHA384                        ECDH         RSA      AES-CBC(256)          SHA384
RSA-AES128-SHA256                              RSA          RSA      AES-CBC(128)          SHA256
RSA-AES256-SHA256                              RSA          RSA      AES-CBC(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}

Ports: 000.000.193.54:25

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                          Code             KEX          Auth     Encryption            MAC
----------------------        ----------       ---          ----     --------------------  ---
DES-CBC3-SHA                                   RSA          RSA      3DES-CBC(168)         SHA1

High Strength Ciphers (>= 112-bit key)

Name                          Code             KEX          Auth     Encryption            MAC
----------------------        ----------       ---          ----     --------------------  ---
ECDHE-RSA-AES128-SHA                           ECDH         RSA      AES-CBC(128)          SHA1
ECDHE-RSA-AES256-SHA                           ECDH         RSA      AES-CBC(256)          SHA1
AES128-SHA                                     RSA          RSA      AES-CBC(128)          SHA1
AES256-SHA                                     RSA          RSA      AES-CBC(256)          SHA1
RC4-MD5                                        RSA          RSA      RC4(128)              MD5
RC4-SHA                                        RSA          RSA      RC4(128)              SHA1
ECDHE-RSA-AES128-SHA256                        ECDH         RSA      AES-CBC(128)          SHA256
ECDHE-RSA-AES256-SHA384                        ECDH         RSA      AES-CBC(256)          SHA384

The fields above are :

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

Unix Operating System Unsupported Version Detection

Plugin ID	**33850**
Family	**General**
Exploit Available	**false**
Severity	**CRITICAL**

ThreadStone explanation:

The operating system (Unix) on the external host is no longer supported. Consider upgrading it.

Synopsis:

The operating system running on the remote host is no longer supported.

Solution:

Upgrade to a version of the Unix operating system that is currently supported.

Host:

000.000.193.24

Plugin output:

```
Ports: 000.000.193.24

FreeBSD 12.2 support ended on 2022-03-31.
Upgrade to FreeBSD 13 / 13.2 / 14 / 14.0.

For more information, see : https://www.freebsd.org/security/
```

Cisco ASA / IOS IKE Fragmentation Vulnerability

Plugin ID	**89033**
Family	**CISCO**
Exploit Available	**true**
Severity	**CRITICAL**

ThreadStone explanation:

The external device is missing a security update for Cisco ASA/IOS IKE, resulting in multiple vulnerabilities. Consider updating it.

Synopsis:

The remote device is missing a vendor-supplied security patch.

Solution:

Upgrade to the relevant fixed version referenced in Cisco Security Advisories cisco-sa-20160210-asa-ike and cisco-sa-20160323-ios-ikev2.

Host:

000.000.193.248

See also:

http://www.nessus.org/u?eafc4e71
http://www.nessus.org/u?9feec3b3
https://www.tenable.com/security/research/tra-2016-06

Plugin output:

Associated CVE's

CVE ID	Severity
CVE-2016-1287	HIGH
CVE-2016-1344	HIGH

SSL Medium Strength Cipher Suites Supported (SWEET32)

Plugin ID	**42873**
Family	**General**
Exploit Available	**false**
Severity	**HIGH**

ThreadStone explanation:

The SSL ciphers are outdated; it is best to update them.

Synopsis:

The remote service supports the use of medium strength SSL ciphers.

Solution:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Host:

000.000.193.139, 000.000.193.151, 000.000.193.151, 000.000.193.168, 000.000.193.45, 000.000.193.54, 000.000.193.31, 000.000.193.191, 000.000.193.68

See also:

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Plugin output:

```
Ports: 000.000.193.31:443

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                          Code             KEX          Auth     Encryption             MAC
----------------------        ----------       ---          ----     --------------------   ---
EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH           RSA      3DES-CBC(168)          SHA1
ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH         RSA      3DES-CBC(168)          SHA1
DES-CBC3-SHA                  0x00, 0x0A       RSA          RSA      3DES-CBC(168)          SHA1

The fields above are :

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

Ports: 000.000.193.139:443, 000.000.193.151:7448, 000.000.193.151:7447, 000.000.193.168:444,
000.000.193.45:1433, 000.000.193.54:25, 000.000.193.191:3389, 000.000.193.68:26

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                          Code             KEX          Auth     Encryption             MAC
----------------------        ----------       ---          ----     --------------------   ---
DES-CBC3-SHA                  0x00, 0x0A       RSA          RSA      3DES-CBC(168)          SHA1

The fields above are :

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

Associated CVE's

CVE ID	Severity
CVE-2016-2183	MEDIUM

Microsoft Exchange Client Access Server Information Disclosure

Plugin ID	**77026**
Family	**Windows**
Exploit Available	**false**
Severity	**HIGH**

ThreadStone explanation:

The Microsoft Exchange Client Access Server (CAS) has a vulnerability that can lead to the disclosure of sensitive information. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted GET request to the web server with an empty 'host header'. As a result, the internal IP address of the system may inadvertently be revealed in the response headers. This leak poses risks such as facilitating further attacks, as the internal network structure is exposed, aiding an attacker in planning targeted attacks or bypassing security measures.

Synopsis:

The remote mail server is affected by an information disclosure vulnerability.

Solution:

Only attack two (Reverse Proxy / Gateway) is fixed in current versions. Apply the latest supplied vendor patches.

Host:

000.000.193.113

See also:

http://foofus.net/?p=758
http://www.nessus.org/u?4eedfe2d

Plugin output:

Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)

Plugin ID	**81649**
Family	**Web Servers**
Exploit Available	**true**
Severity	**HIGH**

Synopsis:

The remote Apache Tomcat server is affected by multiple vulnerabilities.

Solution:

Update to Apache Tomcat version 6.0.43 or later.

Host:

000.000.193.170

See also:

http://tomcat.apache.org/tomcat-6.0-doc/changelog.html
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Plugin output:

```
Ports: 000.000.193.170:80

Installed version : 6.0.35
Fixed version     : 6.0.43
```

Associated CVE's

CVE ID	Severity
CVE-2010-5298	MEDIUM
CVE-2014-0195	MEDIUM
CVE-2014-0198	MEDIUM
CVE-2014-0221	MEDIUM
CVE-2014-0224	MEDIUM
CVE-2014-3470	MEDIUM
CVE-2014-3505	MEDIUM
CVE-2014-3506	MEDIUM
CVE-2014-3507	MEDIUM
CVE-2014-3508	MEDIUM
CVE-2014-3509	MEDIUM
CVE-2014-3510	MEDIUM
CVE-2014-3511	MEDIUM
CVE-2014-3512	HIGH
CVE-2014-3513	HIGH
CVE-2014-3566	MEDIUM
CVE-2014-3567	HIGH
CVE-2014-3568	MEDIUM
CVE-2014-5139	MEDIUM

phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)

Plugin ID	**138595**
Family	**CGI abuses**
Exploit Available	**true**
Severity	**HIGH**

ThreadStone explanation:

The remotely hosted web server is running a PHP application that is vulnerable to SQL injection. Consider updating phpMyAdmin.

Synopsis:

The remote web server hosts a PHP application that is affected by a SQL injection vulnerability.

Solution:

Upgrade to phpMyAdmin version 4.9.4, 5.0.1, or later. Alternatively, apply the patches referenced in the vendor advisories.

Host:

000.000.193.32

See also:

https://www.phpmyadmin.net/security/PMASA-2020-1/

Plugin output:

```
Ports: 000.000.193.32:80

URL               : http://178.255.193.32/phpmyadmin
Installed version : 4.5.4.1deb2ubuntu2.1
Fixed version     : 4.9.4
```

Associated CVE's

CVE ID	Severity
CVE-2020-5504	MEDIUM

HSTS Missing From HTTPS Server (RFC 6797)

Plugin ID	**142960**
Family	**Web Servers**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

If a web application has not implemented the HSTS header, it may be vulnerable to Man-in-the-Middle (MiTM) attacks. An attacker could intercept and manipulate the traffic between the browser and the server, potentially gaining access to confidential information or login credentials. Consider introducing this header to enhance security.

Synopsis:

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

Solution:

Configure the remote web server to use HSTS.

Host:

000.000.193.112, 000.000.193.151, 000.000.193.151, 000.000.193.31, 000.000.193.20

See also:

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

Plugin output:

```
Ports: 000.000.193.31:443

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 01 Jul 2024 22:16:45 GMT
Connection: close
Content-Length: 315


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

Ports: 000.000.193.151:7448, 000.000.193.151:7447

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 01 Jul 2024 22:15:36 GMT
Connection: close
Content-Length: 315


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

Ports: 000.000.193.112:443

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 12 Apr 2021 09:13:09 GMT
Accept-Ranges: bytes
ETag: "ea303de7c2fd71:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 01 Jul 2024 22:15:49 GMT
Connection: close
Content-Length: 703


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

Ports: 000.000.193.20:8843

HTTP/1.1 400
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 435
Date: Mon, 01 Jul 2024 22:12:30 GMT
Connection: close


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

SSL Certificate Cannot Be Trusted

Plugin ID	**51192**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

When a web browser connects to a website with an SSL certificate, the browser checks whether the certificate can be trusted. If the certificate of a website cannot be verified, for instance, because it has expired, been revoked, or issued by an untrusted CA, the browser will warn the user that the connection is not secure. If an attacker manages to fake or hijack a website's SSL certificate, they can intercept, view, and even manipulate the data transmitted between the browser and the server. This can lead to data theft, identity theft, or other forms of cybercrime. To prevent this vulnerability, it is important that SSL certificates are up-to-date and issued by a trusted CA.

Synopsis:

The SSL certificate for this service cannot be trusted.

Solution:

Purchase or generate a proper SSL certificate for this service.

Host:

000.000.193.139, 000.000.193.244, 000.000.193.244, 000.000.193.45, 000.000.193.54, 000.000.193.189, 000.000.193.50, 000.000.193.57, 000.000.193.84

See also:

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Plugin output:

```
Ports: 000.000.193.84:990

The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : OU=Domain Control Validated/OU=PositiveSSL Wildcard/CN=*.freshtandartsen.nl
|-Not After : Jan 02 23:59:59 2021 GMT

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 : OU=Domain Control Validated/OU=PositiveSSL Wildcard/CN=*.freshtandartsen.nl
|-Issuer  : C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation
Secure Server CA

Ports: 000.000.193.45:1433

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=SSL_Self_Signed_Fallback
|-Issuer  : CN=SSL_Self_Signed_Fallback

Ports: 000.000.193.244:4433

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 : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-
```

```
ca2/E=support@fortinet.com
|-Issuer  : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-
ca2/E=support@fortinet.com

Ports: 000.000.193.57:26

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=EXCHANGE01
|-Issuer  : CN=EXCHANGE01

Ports: 000.000.193.189:21

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=*.bernardsanders.com
|-Issuer  : C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure
Server CA

Ports: 000.000.193.54:25

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=Exchange01
|-Issuer  : CN=Exchange01

Ports: 000.000.193.244:444, 000.000.193.50:8843

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=*.optisport.nl
|-Issuer  : C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure
Server CA
```

SSL Self-Signed Certificate

Plugin ID	**57582**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The SSL certificate is not signed by a recognized certificate authority. As a result, the browser views the site as insecure. Consider purchasing an SSL certificate.

Synopsis:

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Solution:

Purchase or generate a proper SSL certificate for this service.

Host:

000.000.193.139, 000.000.193.244, 000.000.193.45, 000.000.193.54, 000.000.193.57

Plugin output:

```
Ports: 000.000.193.57:26

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=EXCHANGE01

Ports: 000.000.193.244:4433

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-
ca2/E=support@fortinet.com

Ports: 000.000.193.45:1433

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=SSL_Self_Signed_Fallback

Ports: 000.000.193.54:25

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=Exchange01
```

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Plugin ID	**65821**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The term "SSL RC4 Cipher Suites Supported (Bar Mitzvah)" refers to a security issue where the use of the outdated RC4 encryption method in SSL/TLS introduces vulnerabilities, specifically an attack known as "Bar Mitzvah." This vulnerability allows an attacker to intercept and decrypt encrypted information. Disable RC4 cipher suites in your SSL/TLS configuration and use modern, more secure encryption methods.

Synopsis:

The remote service supports the use of the RC4 cipher.

Solution:

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Host:

000.000.193.139, 000.000.193.168, 000.000.193.54, 000.000.193.31, 000.000.193.191, 000.000.193.68

See also:

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Plugin output:

```
Ports: 000.000.193.168:444, 000.000.193.54:25, 000.000.193.191:3389, 000.000.193.68:26

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name                          Code            KEX          Auth     Encryption             MAC
----------------------        ----------      ---          ----     --------------------   ---
RC4-MD5                       0x00, 0x04      RSA          RSA      RC4(128)               MD5
RC4-SHA                       0x00, 0x05      RSA          RSA      RC4(128)               SHA1

The fields above are :

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

Ports: 000.000.193.31:443

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name                          Code            KEX          Auth     Encryption             MAC
----------------------        ----------      ---          ----     --------------------   ---
ECDHE-RSA-RC4-SHA             0xC0, 0x11      ECDH         RSA      RC4(128)               SHA1
RC4-MD5                       0x00, 0x04      RSA          RSA      RC4(128)               MD5
RC4-SHA                       0x00, 0x05      RSA          RSA      RC4(128)               SHA1

The fields above are :
```

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

Associated CVE's

CVE ID	Severity
CVE-2013-2566	MEDIUM
CVE-2015-2808	MEDIUM

TLS Version 1.1 Deprecated Protocol

Plugin ID	**157288**
Family	**Service detection**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The TLS version in use is no longer supported. It is best to upgrade to TLS 1.2 or 1.3. In the future, web browsers will consider this connection insecure.

Synopsis:

The remote service encrypts traffic using an older version of TLS.

Solution:

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

Host:

000.000.193.139, 000.000.193.151, 000.000.193.151, 000.000.193.168, 000.000.193.45, 000.000.193.54, 000.000.193.31, 000.000.193.191, 000.000.193.57, 000.000.193.57, 000.000.193.84, 000.000.193.84

See also:

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

Plugin output:

```
Ports: 000.000.193.139:443, 000.000.193.151:7447, 000.000.193.151:7448, 000.000.193.168:444,
000.000.193.45:1433, 000.000.193.54:25, 000.000.193.31:443, 000.000.193.191:3389, 000.000.193.57:587,
000.000.193.57:26, 000.000.193.84:990, 000.000.193.84:21
TLSv1.1 is enabled and the server supports at least one cipher.
```

TLS Version 1.0 Protocol Detection

Plugin ID	**104743**
Family	**Service detection**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The TLS version in use is no longer supported. It is best to upgrade to TLS 1.2 or 1.3. In the future, web browsers will consider this connection insecure.

Synopsis:

The remote service encrypts traffic using an older version of TLS.

Solution:

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

Host:

000.000.193.139, 000.000.193.151, 000.000.193.151, 000.000.193.168, 000.000.193.45, 000.000.193.54, 000.000.193.31, 000.000.193.191, 000.000.193.57, 000.000.193.57, 000.000.193.84, 000.000.193.84

See also:

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Plugin output:

```
Ports: 000.000.193.139:443, 000.000.193.151:7448, 000.000.193.151:7447, 000.000.193.168:444,
000.000.193.45:1433, 000.000.193.54:25, 000.000.193.31:443, 000.000.193.191:3389, 000.000.193.57:26,
000.000.193.57:587, 000.000.193.84:990, 000.000.193.84:21
TLSv1 is enabled and the server supports at least one cipher.
```

Backup Files Disclosure

Plugin ID	**11411**
Family	**CGI abuses**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

It may be possible to retrieve file backups from the external web server.

Synopsis:

It is possible to retrieve file backups from the remote web server.

Solution:

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Host:

000.000.193.244

See also:

http://www.nessus.org/u?8f3302c6

Plugin output:

```
Ports: 000.000.193.244:444

It is possible to read the following backup file :

- File : /logout~
URL  : https://178.255.193.244:444/logout~
```

Apache Tomcat Default Files

Plugin ID	**12085**
Family	**Web Servers**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The Apache Tomcat server has default error pages, default index pages, and sample JSPs or servlets installed. These files pose a risk as they can help an attacker gather information about the Tomcat installation or the host itself. It is advisable to remove these files to prevent potential leaks of sensitive information and reduce the likelihood of a successful attack.

Synopsis:

The remote web server contains default files.

Solution:

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Host:

000.000.193.170

See also:

http://www.nessus.org/u?4cb3b4dd
https://www.owasp.org/index.php/Securing_tomcat

Plugin output:

```
Ports: 000.000.193.170:80

The server is not configured to return a custom page in the event of a client requesting a non-existent
resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

SSL Certificate Expiry

Plugin ID	**15901**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The SSL certificate has expired; consider renewing it. This can lead to reduced website security.

Synopsis:

The remote server's SSL certificate has already expired.

Solution:

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

Host:

000.000.193.113, 000.000.193.84, 000.000.193.84

Plugin output:

```
Ports: 000.000.193.84:990, 000.000.193.84:21

The SSL certificate has already expired :

Subject          : OU=Domain Control Validated, OU=PositiveSSL Wildcard, CN=*.freshtandartsen.nl
Issuer           : C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain
Validation Secure Server CA
Not valid before : Jan  3 00:00:00 2019 GMT
Not valid after  : Jan  2 23:59:59 2021 GMT
```

Apache mod_status /server-status Information Disclosure

Plugin ID	**10677**
Family	**Web Servers**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The Apache web server reveals process information.

Synopsis:

The remote web server discloses process information.

Solution:

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

Host:

000.000.193.36

See also:

https://www.owasp.org/index.php/SCG_WS_Apache

Plugin output:

```
Ports: 000.000.193.36:80

Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://178.255.193.36/server-status

Attached is a copy of the response
```

SMTP Server Non-standard Port Detection

Plugin ID	**18391**
Family	**Backdoors**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

Running an external SMTP service on a non-standard port can pose several risks. First, it may indicate an attempt to bypass security measures or evade monitoring, as standard ports are often monitored for suspicious traffic. This can increase the likelihood of misuse by spammers or attackers. Second, it can cause reliability and compatibility issues, as some networks and firewalls may block traffic on non-standard ports. Lastly, using a non-standard port may require additional management effort to ensure legitimate emails are correctly delivered and received. It is important to weigh the potential benefits against these risks when configuring an SMTP service.

Synopsis:

The remote SMTP service is running on a non-standard port.

Solution:

Check and clean the configuration.

Host:

000.000.193.57

See also:

http://www.icir.org/vern/papers/backdoor/

Plugin output:

```
Ports: 000.000.193.57:26

Banner : 220 EXCHANGE01.sanitas-groep.nl Microsoft ESMTP MAIL Service ready at Tue, 2 Jul 2024 00:12:46
+0200
```

Browsable Web Directories

Plugin ID	**40984**
Family	**CGI abuses**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

Some directories with files on the external web server are publicly visible.

Synopsis:

Some directories on the remote web server are browsable.

Solution:

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Host:

000.000.193.168, 000.000.193.168

See also:

http://www.nessus.org/u?0a35179e

Plugin output:

```
Ports: 000.000.193.168:443

The following directories are browsable :

https://178.255.193.168/services/
https://178.255.193.168/services/Images/
https://178.255.193.168/services/UniteAdminClient/
https://178.255.193.168/services/UniteAlarmAgent/
https://178.255.193.168/services/UniteAssign/
https://178.255.193.168/services/UniteViewClient/

Ports: 000.000.193.168:444

The following directories are browsable :

https://178.255.193.168:444/
```

SSL Certificate with Wrong Hostname

Plugin ID	**45411**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The SSL certificate has an incorrect hostname. For the certificate to be properly trusted, the hostname must be correct, as well as the reverse DNS. This will ensure that users do not encounter errors on their screens. Consider adjusting the hostname.

Synopsis:

The SSL certificate for this service is for a different host.

Solution:

Purchase or generate a proper SSL certificate for this service.

Host:

000.000.193.68

Plugin output:

```
Ports: 000.000.193.68:26

The identities known by Nessus are :

autodiscover.bzhd.nl
webapp.bzhd.nl
hosted.by.qweb.net

The Common Name in the certificate is :

EXCHANGE01

The Subject Alternate Names in the certificate are :

EXCHANGE01
EXCHANGE01.ZHDELTA.LOCAL
```

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

Plugin ID	**62694**
Family	**General**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The external IKEv1 service supports Aggressive Mode with a pre-shared key. Such a key can be leaked and is therefore less secure.

Synopsis:

The remote IKEv1 service supports Aggressive Mode with Pre-Shared key.

Solution:

- Disable Aggressive Mode if supported.
- Do not use Pre-Shared key for authentication if it's possible.
- If using Pre-Shared key cannot be avoided, use very strong keys.
- If possible, do not allow VPN connections from any IP addresses.

Note that this plugin does not run over IPv6.

Host:

000.000.193.113

See also:

http://www.nessus.org/u?8d6444d2
https://www.ernw.de/download/pskattack.pdf
http://www.nessus.org/u?d77bc12e
https://www.securityfocus.com/bid/7423

Plugin output:

Associated CVE's

CVE ID	Severity
CVE-2002-1623	MEDIUM

Web Application Potentially Vulnerable to Clickjacking

Plugin ID	**85582**
Family	**Web Servers**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

Clickjacking is a type of cyberattack where a malicious actor places an invisible or deceptive layer over a legitimate webpage. When a user clicks on the page, believing they are performing a normal action, they are actually clicking on something controlled by the attacker. This can lead to unwanted actions, such as unknowingly sharing personal information or granting access to their computer. Consider implementing the X-Frame-Options header in your web application to prevent your pages from being loaded in malicious iframes.

Synopsis:

The remote web server may fail to mitigate a class of web application vulnerabilities.

Solution:

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

Host:

000.000.193.113, 000.000.193.113, 000.000.193.53

See also:

http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

Plugin output:

```
Ports: 000.000.193.53:444

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- https://178.255.193.53:444/(S(uh4351htpqbv5bxppqgeih31))/Login.aspx
```

Network Time Protocol (NTP) Mode 6 Scanner

Plugin ID	**97861**
Family	**Misc.**
Exploit Available	**false**
Severity	**MEDIUM**

ThreadStone explanation:

The external NTP server responds to mode 6 requests, making it susceptible to a Denial of Service (DoS) attack.

Synopsis:

The remote NTP server responds to mode 6 queries.

Solution:

Restrict NTP mode 6 queries.

Host:

000.000.193.24

See also:

https://ntpscan.shadowserver.org

Plugin output:

```
Ports: 000.000.193.24:123

Nessus elicited the following response from the remote
host by sending an NTP mode 6 query :

'version="ntpd 4.2.8p15@1.3728-o Fri Feb  5 22:07:56 UTC 2021 (1)",
processor="amd64", system="FreeBSD/12.2-STABLE", leap=0, stratum=3,
precision=-20, rootdelay=4.800, rootdisp=21.771, refid=158.101.221.122,
reftime=0xea2da5e2.561f75b2, clock=0xea2da930.ae8b9d61, peer=27439,
tc=9, mintc=3, offset=0.098703, frequency=3.882, sys_jitter=0.139855,
clk_jitter=0.174, clk_wander=0.010'
```

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Plugin ID	**78479**
Family	**General**
Exploit Available	**true**
Severity	**LOW**

ThreadStone explanation:

The host is vulnerable to a Man-in-the-Middle (MitM) attack known as POODLE, due to an issue in how SSL 3.0 processes padding bytes when decrypting messages encrypted with block ciphers in CBC mode. Attackers can exploit this vulnerability to decrypt a selected byte of ciphertext in just 256 attempts, provided they can force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. This poses significant risks to the confidentiality of sensitive information transmitted through these services.

Synopsis:

It is possible to obtain sensitive information from the remote host
with SSL/TLS-enabled services.

Solution:

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV
mechanism until SSLv3 can be disabled.

Host:

000.000.193.139, 000.000.193.53, 000.000.193.54

See also:

https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Plugin output:

```
Ports: 000.000.193.53:444, 000.000.193.54:25

Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

Associated CVE's

CVE ID	Severity
CVE-2014-3566	MEDIUM

ICMP Timestamp Request Remote Date Disclosure

Plugin ID	**10114**
Family	**General**
Exploit Available	**false**
Severity	**LOW**

ThreadStone explanation:

It is possible to determine the exact time set on the external host.

Synopsis:

It is possible to determine the exact time set on the remote host.

Solution:

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Host:

000.000.193.113, 000.000.193.1

Plugin output:

```
Ports: 000.000.193.1
The remote clock is synchronized with the local clock.
```

Associated CVE's

CVE ID	Severity
CVE-1999-0524	LOW

Web Server HTTP Header Internal IP Disclosure

Plugin ID	**10759**
Family	**Web Servers**
Exploit Available	**true**
Severity	**LOW**

ThreadStone explanation:

This web server leaks a private IP address through its HTTP headers, exposing internal IP addresses that are typically hidden or masked behind a Network Address Translation (NAT) firewall or proxy server. This can lead to security risks as attackers can gain insight into the internal structure of the network, paving the way for targeted attacks such as network scanning, port mapping, and exploiting vulnerabilities within the internal network. Leaking this information can also reduce the effectiveness of security measures like IP address verification and undermine the system's anonymity.

Synopsis:

This web server leaks a private IP address through its HTTP headers.

Solution:

Apply configuration suggested by vendor.

Host:

000.000.193.113, 000.000.193.35

See also:

http://www.nessus.org/u?fe24f941
http://www.nessus.org/u?8e23582e
http://www.nessus.org/u?4eedfe2d

Plugin output:

```
Ports: 000.000.193.35:80

Nessus was able to exploit the issue using the following request :

GET / HTTP/1.0
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
Connection: close
Content-Type: text/html
Location: https://10.34.0.46/


------------------------------ snip ------------------------------
```

Associated CVE's

CVE ID	Severity
CVE-2000-0649	LOW

Web Server Transmits Cleartext Credentials

Plugin ID	**26194**
Family	**Web Servers**
Exploit Available	**false**
Severity	**LOW**

ThreadStone explanation:

The web server may transmit login credentials in plain text. It contains multiple HTML form fields with a 'password' input type that send their information unencrypted to an external web server. This poses a significant security risk because unauthorized individuals can easily intercept the sensitive information, especially if the connection does not use HTTPS. It is essential to encrypt all authentication data during transmission to ensure the confidentiality and integrity of user information.

Synopsis:

The remote web server might transmit credentials in cleartext.

Solution:

Make sure that every sensitive form transmits content over HTTPS.

Host:

000.000.193.113

Plugin output:

Web Server Allows Password Auto-Completion

Plugin ID	**42057**
Family	**Web Servers**
Exploit Available	**false**
Severity	**LOW**

ThreadStone explanation:

Not disabling the 'autocomplete' feature on password fields entails certain risks. When a web server contains HTML form fields where 'autocomplete' is not set to 'off' for input fields of type 'password', user data, such as passwords, can be stored in the browser. This does not pose a direct risk to the web server itself but can lead to a loss of confidentiality of user data. This risk is particularly significant when users access the site from shared computers or if their own device becomes compromised at any point.

Synopsis:

The 'autocomplete' attribute is not disabled on password fields.

Solution:

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

Host:

000.000.193.113, 000.000.193.113, 000.000.193.53

Plugin output:

```
Ports: 000.000.193.53:444
Page : /(S(uh4351htpqbv5bxppqgeih31))/Login.aspx
Destination Page: /(S(uh4351htpqbv5bxppqgeih31))/Login.aspx
```

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

Plugin ID	**83875**
Family	**Misc.**
Exploit Available	**false**
Severity	**LOW**

ThreadStone explanation:

The external host allows SSL/TLS connections with Diffie-Hellman moduli of 1024 bits or less. This poses a security risk because, through cryptanalysis, a third party could potentially discover the shared secret in a relatively short time (depending on the size of the modulus and the attacker's resources). This could allow an attacker to intercept plaintext or compromise the integrity of the connections. Using weaker Diffie-Hellman moduli makes the system vulnerable to attacks such as 'Logjam,' where the encryption can be broken and sensitive information compromised.

Synopsis:

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Solution:

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048

bits or greater.

Host:

000.000.193.113, 000.000.193.162, 000.000.193.53

See also:

https://weakdh.org/

Plugin output:

```
Ports: 000.000.193.53:444

Vulnerable connection combinations :

SSL/TLS version  : TLSv1.0
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.0
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.1
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.1
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

Ports: 000.000.193.162:8443

Vulnerable connection combinations :

SSL/TLS version  : TLSv1.2
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.2
Cipher suite     : TLS12_DHE_RSA_WITH_AES_128_GCM_SHA256
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.2
Cipher suite     : TLS12_DHE_RSA_WITH_AES_256_GCM_SHA384
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.2
Cipher suite     : TLS1_DHE_RSA_WITH_AES_128_CBC_SHA256
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)
```

```
SSL/TLS version  : TLSv1.2
Cipher suite     : TLS1_DHE_RSA_WITH_AES_256_CBC_SHA256
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)

SSL/TLS version  : TLSv1.2
Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)
```

Associated CVE's

CVE ID	Severity
CVE-2015-4000	MEDIUM

SSH Weak Key Exchange Algorithms Enabled

Plugin ID	**153953**
Family	**Misc.**
Exploit Available	**false**
Severity	**LOW**

ThreadStone explanation:

An SSH server configured to allow weak key exchange algorithms is at increased risk of traffic interception and decryption by malicious actors. According to the IETF guidelines in the document 'draft-ietf-curdle-ssh-kex-sha2-20,' certain algorithms should no longer be used because they contain vulnerabilities that can compromise the security of the connection. Allowing these outdated or weak algorithms can lead to man-in-the-middle attacks, where an attacker can take control of the data stream, and the cracking of encrypted communication, jeopardizing the integrity and confidentiality of the transmitted data. It is therefore crucial for administrators to update the SSH server configuration to support only strong, recommended key exchange algorithms.

Synopsis:

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

Solution:

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

Host:

000.000.193.191

See also:

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

Plugin output:

```
Ports: 000.000.193.191:22

The following weak key exchange algorithms are enabled :

diffie-hellman-group-exchange-sha1
gss-gex-sha1-toWM5Slw5Ew8Mqkay+al2g==
gss-group14-sha1-toWM5Slw5Ew8Mqkay+al2g==
```