VERTROUWELIJK

RAPPORTAGE THREADSCAN

TECHNISCHE RAPPORTAGE

ALGEMENE INFORMATIE

gescand

Scan op:	score11.threadstone.eu
Datum scan:	10 september 2018
Type scan:	Automatisch

ABONNEMENT INFORMATIE

Type abonnement:	Infra
Scan frequentie:	elke maand
Scan diepte:	n.v.t.

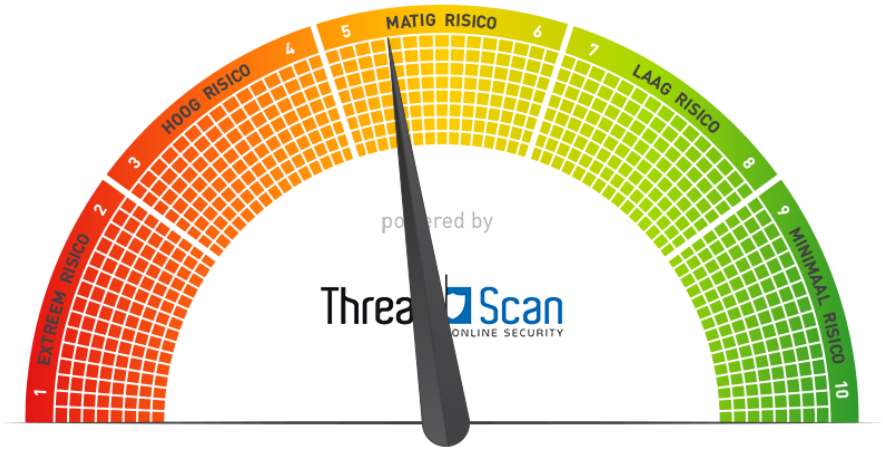
ThreadStone Cyber Security B.V.
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
www.threadstone.eu

T: +31 (0)85 060 7000
M: info@threadstone.eu

Kvk : 614 262 02
BTW nummer: NL 85 43 36 631 B01
IBAN: NL34 RABO 0192 0442 14

ThreadStone Cyber Security kan op geen enkele manier aansprakelijkheid aanvaarden voor de gevolgen van onvolledigheid of onjuistheid van informatie en materiaal dat in dit rapport of de diensten van ThreadStone Cyber Security ter beschikking worden gesteld. Ook kan deze rapportage niet gezien worden als (bindend) advies. Het is niet mogelijk om garanties te bieden op 'compliant' zijn met de Algemene Verordening Gegevensbescherming of andere wetgeving op basis van de diensten of rapportages van ThreadStone Cyber Security.

Met de diensten van ThreadStone Cyber Security wordt u mogelijk verwezen naar andere websites, rapporten en technische oplossingen die niet onder controle staan van ThreadStone Cyber Security. Wij hebben geen controle over de aard, inhoud en de beschikbaarheid van deze bronnen. Daarnaast zijn deze bronnen aan tussentijdse verandering onderhevig, waardoor bepaalde informatie mogelijk niet meer actueel of compleet kan zijn. De opname van welke informatie dan ook is niet noodzakelijkerwijs een aanbeveling of onderschrijving van standpunten die door (andere) bronnen of wetgever worden geuit en hebben slechts een informatieve strekking.



DE SCORE VAN DE THREADSCAN IS: 5* (MATIG RISICO)

Uw website of bedrijfsnetwerk is redelijk beveiligd tegen cyberinbraken, maar er zijn kwetsbaarheden gedetecteerd met een gemiddelde prioriteit. Raadpleeg uw IT'er om te onderzoeken of er risico op dataverlies is en om de geconstateerde kwetsbaarheden weg te nemen.

* Gebaseerd op de score-indeling van ThreadStone

We hebben onderzoek gedaan naar de top-100 kwetsbaarheden die in onze systemen voorkomen op basis van de scans die in het verleden zijn uitgevoerd. Voor deze top-100 hebben we geprobeerd om in begrijpelijke taal te beschrijven wat het probleem exact inhoudt en wat de impact kan zijn op het moment dat misbruik zou worden gemaakt van de kwetsbaarheid. In dit hoofdstuk wordt dit per gevonden kwetsbaarheid beschreven.

Let op! Aangezien deze gegevens uit onze top-100 komt, zal deze lijst waarschijnlijk niet compleet zijn. Voor kwetsbaarheden die als "informatief" zijn geclassificeerd zal bijvoorbeeld geen mogelijke business impact zijn beschreven. Richt u dus niet alleen op deze beschrijvingen, maar neem alle geconstateerde problemen (zie hoofdstuk 'Overzicht van de gevonden kwetsbaarheden') door met uw IT-leverancier!

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

MOGELIJKE BUSINESS IMPACT
Via een man in de middle attack is het mogelijk om het SSL verkeer te decrypten. Hierdoor kan data zoals wachtwoorden of andere gegevens mogelijk onveilig worden verstuurd over het internet.

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

MOGELIJKE BUSINESS IMPACT
Het SSL Certificaat gebruikt een algoritme wat niet sterk genoeg is.

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

MOGELIJKE BUSINESS IMPACT
De website kan worden gekopieerd in een andere websites. Daardoor kunnen gebruikers het idee krijgen dat ze op site A werken terwijl ze de gegevens doorsturen voor site B.

The remote web server might be prone to cross-site request forgery attacks.

MOGELIJKE BUSINESS IMPACT
Het is wellicht mogelijk om misbruik te maken van de formulieren op de website omdat een security token ontbreekt. Een security token op de formulieren verhoogd de beveiliging.

ADVIES
Plaats een security token op de formulieren.

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

MOGELIJKE BUSINESS IMPACT
Het SSL Certificaat wordt niet vertrouwd, hierdoor kunnen gebruikers denken dat de server niet valide is en besluiten geen gebruik te maken van deze server/website.

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled service

MOGELIJKE BUSINESS IMPACT
Via een man in de middle attack is het mogelijk om het SSL verkeer te decrypten. Hierdoor kan data zoals wachtwoorden of andere gegevens mogelijk onveilig worden verstuurd over het internet.

An insecure port, protocol or service has been detected.

MOGELIJKE BUSINESS IMPACT
Het email verkeer gaat via een onveilig protocol. Dit betekent dat het verkeer kan worden onderschept en eventueel worden gemanipuleerd

---

The SSL certificate for this service cannot be trusted.

MOGELIJKE BUSINESS IMPACT
Het SSL Certificaat wordt niet vertrouwd, hierdoor kunnen gebruikers denken dat de server niet valide is en besluiten geen gebruik te maken van deze server/website.

A remote access software has been detected.

MOGELIJKE BUSINESS IMPACT
Het is mogelijk om op deze server vanaf afstand in te loggen. Dit kan de bedoeling zijn maar brengt ook risico`s met zich mee

---

The remote service supports the use of 64-bit block ciphers.

MOGELIJKE BUSINESS IMPACT
Het SSL Certificaat gebruikt een algoritme wat niet sterk genoeg is.

Kwetsbaarheden met kritieke prioriteit:	0
Kwetsbaarheden met hoge prioriteit:	0
Kwetsbaarheden met medium prioriteit:	10
Kwetsbaarheden met lage prioriteit:	0
Informatieve meldingen:	12
Scan afgebroken door firewall of Intrusion detection systeem:	NEE

GEVONDEN KWETSBAARHEDEN MET MEDIUM PRIORITEIT

BESCHRIJVING	CVSS SCORE*	EXPLOIT BESCHIKBAAR
The remote service encrypts traffic using a protocol with known weaknesses.	5,0	-
The remote service supports the use of medium strength SSL ciphers.	4,3	-
The remote web server fails to mitigate a class of web application vulnerabilities.	4,3	-
The remote web server might be prone to cross-site request forgery attacks.	6,4	-
The SSL certificate for this service is for a different host.	5,0	-
It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled service	4,3	Ja
An insecure port, protocol or service has been detected.	-	-
The SSL certificate for this service cannot be trusted.	6,4	-
A remote access software has been detected.	-	-
The remote service supports the use of 64-bit block ciphers.	2,6	Ja

* voor nadere uitleg over de CVSS score en de betekenis van exploits verwijzen we naar hoofdstuk "Score kwetsbaarheden conform CVSS"

INFORMATIEVE MELDINGEN

Onze scans krijgen op verzoeken die we uitvoeren reactie terug. Dit kan bijvoorbeeld zijn dat op een website documenten gevonden zijn. Of het de bedoeling is dat deze documenten vanaf de website worden gedeeld is niet door onze scanners te bepalen; dit zal nader onderzocht moeten worden. Dit soort meldingen worden als informatieve meldingen weergegeven en hebben daarom veelal geen CVSS scoring. Wij adviseren wel om uw IT'er ook deze meldingen te laten analyseren.

BESCHRIJVING
The remote service encrypts communications.
The remote service could be identified.
It is possible to determine which TCP ports are open.
Some information about the remote HTTP configuration can be extracted.
A web server is running on the remote host.
This plugin determines which HTTP methods are allowed on various CGI directories.
The remote web server does not return 404 error codes.
According to the DNS, DNSSEC is not enabled.
According to the DNS, your hosting provider doesn't have IPv6 enabled on the DNS Server.
According to Phishtank, your site is not being used for phishing.
According to Web of Trust, your site is not rated or rated as reliable.
No malware found on google safebrowsing.

THE REMOTE SERVICE ENCRYPTS TRAFFIC USING A PROTOCOL WITH KNOWN WEAKNESSES.

TOP 100

OMSCHRIJVING

The remote service accepts connections encrypted using TLS 1.0. This version of TLS is affected by multiple cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

OPLOSSING

All processing and third party entities - including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater service offering by June 2016. All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective June 2018.

GEDETAILLEERDE INFORMATIE

Port: 443

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

Plugin Details

Severity	Medium
PluginID	84470
Version	$Revision: 1.3 $
Type	remote
Family	Service detection
Published	2015/06/30
Modified	2016/05/26

Risk information

Risk factor	Medium
CVSS Base Score	5.0

THE REMOTE SERVICE SUPPORTS THE USE OF MEDIUM STRENGTH SSL CIPHERS.

OMSCHRIJVING

The remote host supports the use of SSL ciphers that offer medium strength encryption. ThreadScan regards medium strength as any encryption that uses key lengths at least 56 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

OPLOSSING

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

GEDETAILLEERDE INFORMATIE

Port: 443

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

Medium Strength Ciphers (> 64-bit and < 112-bit key)

TLSv1
DES-CBC3-SHA                Kx=RSA          Au=RSA       Enc=3DES-CBC(168)         Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

Plugin Details

Severity	Medium
PluginID	42873
Version	$Revision: 1.15 $
Type	remote
Family	General
Published	2009/11/23
Modified	2016/12/30

Risk information

Risk factor	Medium
CVSS Base Score	4.3

THE REMOTE WEB SERVER FAILS TO MITIGATE A CLASS OF WEB APPLICATION VULNERABILITIES.

TOP 100

OMSCHRIJVING

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

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

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

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

OPLOSSING

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.

GEDETAILLEERDE INFORMATIE

Port: 444

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

- https://score11.threadstone.eu/manual/
- https://score11.threadstone.eu/manual/de/
```

Plugin Details

Severity	Medium
PluginID	85582
Version	$Revision: 1.5 $
Type	remote
Family	Web Servers
Published	2015/08/22
Modified	2016/06/13

Risk information

Risk factor	Medium
CVSS Base Score	4.3

THE REMOTE WEB SERVER MIGHT BE PRONE TO CROSS-SITE REQUEST FORGERY ATTACKS.

TOP 100

OMSCHRIJVING

The spider found HTML forms on the remote web server. Some CGI scripts do not appear to be protected by random tokens, a common anti-cross-site request forgery (CSRF) protection. The web application might be vulnerable to CSRF attacks.

Note that :

- ThreadScan did not exploit the flaw,
- ThreadScan cannot identify sensitive actions -- for example, on an online bank, consulting an account is less sensitive than transferring money.

You will have to audit the source of the CGI scripts and check if they are actually affected.

OPLOSSING

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

GEDETAILLEERDE INFORMATIE

Port: 443

```
The following CGIs are not protected by a random token :
/CMSPages/logon.aspx?ReturnUrl=%2fCMSModules
```

Plugin Details

Severity	Medium
PluginID	56818
Version	$Revision: 1.6 $
Type	remote
Family	CGI abuses
Published	2011/11/17
Modified	2014/12/30

Risk information

Risk factor	Medium
CVSS Base Score	6.4

THE SSL CERTIFICATE FOR THIS SERVICE IS FOR A DIFFERENT HOST.

OMSCHRIJVING

The commonName (CN) of the SSL certificate presented on this service is for a different machine.

OPLOSSING

Purchase or generate a proper certificate for this service.

GEDETAILLEERDE INFORMATIE

Port: 443

```
The identity known by ThreadScan is :

score11.threadstone.eu

The Common Name in the certificate is :

localhost

The Subject Alternate Names in the certificate are :

localhost.local
```

Plugin Details

Severity	Medium
PluginID	45411
Version	1.15
Type	remote
Family	General
Published	2010/04/03
Modified	2014/03/11

Risk information

Risk factor	Medium
CVSS Base Score	5.0

IT MAY BE POSSIBLE TO OBTAIN SENSITIVE INFORMATION FROM THE REMOTE HOST WITH SSL/TLS-ENABLED SERVICE

TOP 100

OMSCHRIJVING

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.
If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

OPLOSSING

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.
Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

GEDETAILLEERDE INFORMATIE

Port: 443

```
Negotiated cipher suite: AES256-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES-CBC(256)|Mac=SHA1
```

Plugin Details

Severity	Medium
PluginID	58751
Version	1.23
Type	remote
Family	General
Published	2012/04/16
Modified	2015/11/30

Risk information

Risk factor	Medium
CVSS Base Score	4.3

AN INSECURE PORT, PROTOCOL OR SERVICE HAS BEEN DETECTED.

TOP 100

OMSCHRIJVING

Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. An attacker who is able to exploit weak cryptographic processes can gain control of an application or even gain cleartext access to encrypted data.

OPLOSSING

Properly encrypt all authenticated and sensitive communications.

GEDETAILLEERDE INFORMATIE

Port: 80

```
Page : /Login/portal/Login.aspx
Destination Page: /Login/portal/Login.aspx
```

Plugin Details

Severity	Medium
PluginID	56208
Version	$Revision: 1.6 $
Type	remote
Family	Policy Compliance
Published	2011/09/15
Modified	2016/01/05

Risk information

Risk factor	Medium
CVSS Base Score	-

THE SSL CERTIFICATE FOR THIS SERVICE CANNOT BE TRUSTED.

TOP 100

OMSCHRIJVING

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that ThreadScan either does not support or does not recognize.

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

OPLOSSING

Purchase or generate a proper certificate for this service.

GEDETAILLEERDE INFORMATIE

Port: 443

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

|-Subject : OU=Domain Control Validated/OU=invalid/CN=score11.threadstone.eu
|-Issuer  : C=GB/ST=invalid/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure
Server CA
```

Plugin Details

Severity	Medium
PluginID	51192
Version	$Revision: 1.14 $
Type	remote
Family	General
Published	2010/12/15
Modified	2015/10/21

Risk information

Risk factor	Medium
CVSS Base Score	6.4

A REMOTE ACCESS SOFTWARE HAS BEEN DETECTED.

OMSCHRIJVING

Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D in the ASV Program Guide, or disabled / removed. Please consult your ASV if you have questions about this Special Note.

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 0

```
An IKEv1 server (VPN) is running on the remote host on UDP port 500.
```

Plugin Details

Severity	Medium
PluginID	56209
Version	1.19
Type	summary
Family	Policy Compliance
Published	2011/09/15
Modified	2015/12/17

Risk information

Risk factor	Medium
CVSS Base Score	-

THE REMOTE SERVICE SUPPORTS THE USE OF 64-BIT BLOCK CIPHERS.

OMSCHRIJVING

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

OPLOSSING

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers.

GEDETAILLEERDE INFORMATIE

Port: 443

```
List of 64-bit block cipher suites supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key)

TLSv1
DES-CBC3-SHA                Kx=RSA          Au=RSA      Enc=3DES-CBC(168)         Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

Plugin Details

Severity	Medium
PluginID	94437
Version	$Revision: 1.3 $
Type	remote
Family	General
Published	2016/11/01
Modified	2016/12/14

Risk information

Risk factor	Low
CVSS Base Score	2.6

THE REMOTE SERVICE ENCRYPTS COMMUNICATIONS.

OMSCHRIJVING

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

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 443

This port supports TLSv1.0/TLSv1.1/TLSv1.2.

Plugin Details

Severity	Informatie
PluginID	56984
Version	1.19
Type	remote
Family	General
Published	2011/12/01
Modified	2016/01/11

Risk information

Risk factor	None
CVSS Base Score	-

THE REMOTE SERVICE COULD BE IDENTIFIED.

OMSCHRIJVING

ThreadScan 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.

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 443

A web server is running on this port through TLSv1.

Port: 443

A TLSv1 server answered on this port.

Port: 80

A web server is running on this port.

Plugin Details

Severity	Informatie
PluginID	22964
Version	$Revision: 1.156 $
Type	remote
Family	Service detection
Published	2007/08/19
Modified	2017/05/26

Risk information

Risk factor	None
CVSS Base Score	-

IT IS POSSIBLE TO DETERMINE WHICH TCP PORTS ARE OPEN.

OMSCHRIJVING

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.

OPLOSSING

Protect your target with an IP filter.

GEDETAILLEERDE INFORMATIE

Port: 443

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

Port: 80

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

Plugin Details

Severity	Informatie
PluginID	11219
Version	$Revision: 1.24 $
Type	remote
Family	Port scanners
Published	2009/02/04
Modified	2017/05/22

Risk information

Risk factor	None
CVSS Base Score	-

SOME INFORMATION ABOUT THE REMOTE HTTP CONFIGURATION CAN BE EXTRACTED.

OMSCHRIJVING

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

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

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 80

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

Server: nginx
Date: Thu, 01 Jun 2017 03:26:40 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: https://score11.threadstone.eu/
```

Plugin Details

Severity	Informatie
PluginID	24260
Version	$Revision: 1.12 $
Type	remote
Family	Web Servers
Published	2007/01/30
Modified	2011/05/31

Risk information

Risk factor	None
CVSS Base Score	-

A WEB SERVER IS RUNNING ON THE REMOTE HOST.

OMSCHRIJVING

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

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 80

```
The remote web server type is :

nginx
```

Plugin Details

Severity	Informatie
PluginID	10107
Version	$Revision: 1.123 $
Type	remote
Family	Web Servers
Published	2000/01/04
Modified	2016/02/19

Risk information

Risk factor	None
CVSS Base Score	-

THIS PLUGIN DETERMINES WHICH HTTP METHODS ARE ALLOWED ON VARIOUS CGI DIRECTORIES.

OMSCHRIJVING

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

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.

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 80

```
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 MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/
```

Plugin Details

Severity	Informatie
PluginID	43111
Version	$Revision: 1.7 $
Type	remote
Family	Web Servers
Published	2009/12/10
Modified	2013/05/09

Risk information

Risk factor	None
CVSS Base Score	-

THE REMOTE WEB SERVER DOES NOT RETURN 404 ERROR CODES.

OMSCHRIJVING

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

ThreadScan has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

OPLOSSING

n/a

GEDETAILLEERDE INFORMATIE

Port: 80

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

http://score11.threadstone.eu/f7EfKgjxdY57.html
```

Plugin Details

Severity	Informatie
PluginID	10386
Version	$Revision: 1.98 $
Type	remote
Family	Web Servers
Published	2000/04/28
Modified	2015/10/13

Risk information

Risk factor	None
CVSS Base Score	-

ACCORDING TO THE DNS, DNSSEC IS NOT ENABLED.

OMSCHRIJVING

DNSSEC provides extra security features for your domain. With DNSSEC enabled the user gets an extra digital signature that prooves the authenticity of the domain.

OPLOSSING

Contact your hosting provider to check if DNSSEC can be enabled.

GEDETAILLEERDE INFORMATIE

Port: 0

```
LOW: Domain has no DNSSEC
```

Plugin Details

Severity	Informatie
PluginID	750801
Version	Version 1.0
Type	remote
Family	CGI abuses
Published	2017/01/16
Modified	2017/01/16

Risk information

Risk factor	None
CVSS Base Score	-

ACCORDING TO THE DNS, YOUR HOSTING PROVIDER DOESN'T HAVE IPV6 ENABLED ON THE DNS SERVER.

OMSCHRIJVING

With IPv6 enabled you are ready for the new internet standard.

OPLOSSING

Contact your hosting provider to check if IPv6 can be enabled on their DNS server

GEDETAILLEERDE INFORMATIE

Port: 0

```
LOW: No nameserver has an AAAA record
```

Plugin Details

Severity	Informatie
PluginID	750805
Version	Version 1.0
Type	remote
Family	CGI abuses
Published	2017/01/16
Modified	2017/01/16

Risk information

Risk factor	None
CVSS Base Score	-

ACCORDING TO PHISHTANK, YOUR SITE IS NOT BEING USED FOR PHISHING.

OMSCHRIJVING

Phishtank is a free community site where users can submit, verify, track and share phishing data. The list is updated on a daily basis

OPLOSSING

In case you believe there is false positive or if you have removed the phishing details from your website check the faq on phishtank.com to report it.

GEDETAILLEERDE INFORMATIE

Port: 0

```
INFO, score11.threadstone.eu is not in the list of www.phistank.com
```

Plugin Details

Severity	Informatie
PluginID	750200
Version	Version 1.0
Type	remote
Family	CGI abuses
Published	2017/01/16
Modified	2017/01/16

Risk information

Risk factor	None
CVSS Base Score	-

ACCORDING TO WEB OF TRUST, YOUR SITE IS NOT RATED OR RATED AS RELIABLE.

OMSCHRIJVING

Web of Trust detects if your website is rated as unreliable. The rating is calculated through a combination of user ratings and data from other sources.

OPLOSSING

Web of Trust is based on user ratings. In case no rating or a bad ratings exists check the FAQ on Web of Trust to get more ratings https://www.mywot.com/en/faq .

GEDETAILLEERDE INFORMATIE

Port: 0

```
INFO, score11.threadstone.eu has a good rating according to Web of Trust : http://www.mywot.com
```

Plugin Details

Severity	Informatie
PluginID	750100
Version	Version 1.0
Type	remote
Family	CGI abuses
Published	2017/01/16
Modified	2017/01/16

Risk information

Risk factor	None
CVSS Base Score	-

NO MALWARE FOUND ON GOOGLE SAFEBROWSING.

OMSCHRIJVING

Google Safe Browsing is a Google service that checks your URL against Google's constantly updated lists of suspected phishing, malware, and unwanted software pages.

OPLOSSING

In case your site is blacklisted or contains malware you can contact Google to check your site again via http://www.google.com/webmasters/tools/

GEDETAILLEERDE INFORMATIE

Port: 0

```
INFO, score11.threadstone.eu is considered safe according to Google Safe Browsing.
```

Plugin Details

Severity	Informatie
PluginID	750300
Version	Version 1.0
Type	remote
Family	CGI abuses
Published	2017/01/16
Modified	2017/01/16

Risk information

Risk factor	None
CVSS Base Score	-

Warranty and waiver

Dit rapport bevat uitkomsten over de ThreadScan die is verricht door ThreadStone Cyber Security B.V. (hierna: "ThreadStone"). De vrijwaringsverklaring en gebruikersvoorwaarden zijn van toepassing op de diensten van ThreadStone.

ThreadScan controleert standaard op kwetsbaarheden die vanaf het externe netwerk zichtbaar zijn (een zgn. outside-in scan). Dit betekent dat het rapport alle en kwetsbaarheden opsomt die vanaf het internet detecteerbaar zijn. De scans worden uitgevoerd op een veilige manier; dit betekent dat (Distributed) Denial of service-aanvallen ((D)DoS-aanvallen) niet in de scan worden uitgevoerd.

ThreadStone voert de scans uit vanaf een serverpark in Duitsland en Nederland. De scans zijn uitgevoerd vanuit de IP adressen 78.46.19.149 en 5.9.17.13. Zorg er voor dat deze IP nummers op de "allow" list staan van uw firewalls.

Indien u een firewall gebruikt die alle contactpogingen in logbestanden plaatst, dan zullen de scans vanaf onze IP-adressen in de logs terugkomen. De logmeldingen waarin onze IP adressen zijn genoemd zijn afkomstig van de servers van ThreadStone Cyber Security en zijn OP GEEN ENKELE WIJZE EEN POGING TOT INBRAAK OF POGING TOT TOEBRENGEN VAN SCHADE. U kunt de logbestanden zien als handige informatie dat uw detectiesystemen juist functioneren, maar wees niet bezorgd over het verschijnen van deze logs in uw firewall. Dit is het juiste gedrag van uw systemen.

ThreadStone is een Cyber Security bedrijf dat veiligheid scans (vulnerability scans) en penetratie testen uitvoert. ThreadStone heeft certificeringen als EC Council Licenced penetratie tester, Certified Ethical hacker en Certified security analyst. De scans worden met de grootste zorg en uiterste precisie uitgevoerd. Wij kunnen echter geen garanties geven voor wat betreft de inhoud of volledigheid van dit rapport.

CyberStatus, ThreadScan en ThreadStone zijn handelsmerken van ThreadStone Cyber Security B.V.. Alle andere product- en bedrijfsnamen zijn handelsmerken of geregistreerde handelsmerken van andere partijen.

Met dit verslag wordt u mogelijk verwezen naar andere websites, rapporten en technische oplossingen die niet onder de controle staan van ThreadStone. Wij hebben daarom geen controle over de aard, inhoud en de beschikbaarheid van deze bronnen. Daarnaast zijn deze bronnen aan tussentijdse verandering onderhevig, waardoor bepaalde informatie mogelijk niet meer actueel en compleet kan zijn. De opname van welke informatie dan ook is niet noodzakelijkerwijs een aanbeveling of onderschrijving van standpunten die door andere bronnen worden geuit en hebben slechts een informatieve strekking.

De scans worden met de grootste zorg en uiterste precisie uitgevoerd. Leverancier kan echter geen garanties geven voor wat betreft de inhoud of volledigheid van dit rapport.

Uitleg betekenis CVSS score

De geconstateerde kwetsbaarheden worden gekwalificeerd conform de score van CVSS. Dit is een vrije en open industriestandaard voor de beoordeling van de ernst van kwetsbaarheden in computersystemen en websites. De standaard is onder beheer van het Forum of Incident Response and Security Teams (FIRST).

CVSS kwalificeert kwetsbaarheden op risico in vergelijking met andere kwetsbaarheden, zodat benodigde inspanningen vervolgens kunnen worden geprioriteerd. De scores zijn gebaseerd op een aantal metingen (metriek genoemd) op basis van evaluatie door deskundigen. De scores lopen van 0 tot 10. Beveiligingsproblemen met een basisscore in het bereik 9.0-10.0 zijn kritisch, die in het bereik 7.0-8,9 zijn hoog, 4.0-6,9 zijn medium en 0.1-3.9 zijn laag.

Voor de volledigheid worden ook de informatieve berichten (score 0) geregistreerd en gerapporteerd.

De ThreadScan vertaalt de CVSS score automatisch naar een eigen score, gebaseerd op de kwetsbaarheid met de hoogste score op CVSS.

Score conform CVSS

Critical	9.0..10.0
High	7.0..8.9
Medium	4.0..6.9
Low	0.1..3.9
Information	0

Uitleg betekenis 'Exploit beschikbaar'

Met behulp van een exploit kan een kwaadwillend persoon misbruik maken van een kwetsbaarheid in uw website of bedrijfsnetwerk. Een exploit is een klein programma waarmee iemand via een kwetsbaarheid bijvoorbeeld toegang kan krijgen tot uw systeem. Exploits voor bekende kwetsbaarheden zijn soms ook makkelijk te vinden op het internet. In het overzicht van kwetsbaarheden wordt per kwetsbaarheid aangegeven of er exploits bekend zijn. Dit betekent niet direct dat uw website of bedrijfsnetwerk reeds misbruikt is; het geeft aan dat uw website of bedrijfsnetwerk - over het algemeen - relatief eenvoudig misbruikt kán worden.

Wat geeft mijn score aan?

De kwetsbaarheden worden geprioriteerd conform de internationale open industrie standaard: CVSS. De CVSS-score geeft een onafhankelijke weging aan een kwetsbaarheid op basis waarvan de kwetsbaarheden worden gewogen. De getoonde rapportcijfers zijn afgeleid van de CVSS-score op basis van deze tabel.

Let op: Werken aan uw digitale veiligheid is nooit klaar. Zelfs als u een 10 scoort bent u niet 100% veilig. Hackers vinden namelijk steeds nieuwe manieren om uw beveiliging te doorbreken. U zal dus voortdurend moeten blijven investeren in uw veiligheid.

SCORE 1-2 Extreem risico

(Urgente actie door uw IT'er vereist)

Uw website of bedrijfsnetwerk staat open voor cyberinbraken. We hebben kwetsbaarheden ontdekt met een kritieke urgentie. Raadpleeg uw IT'er met urgentie om te onderzoeken of er risico op dataverlies is en om de geconstateerde kwetsbaarheden weg te nemen.

SCORE 3-4 Hoog risico

(Directe actie door uw IT'er nodig)

Uw website of bedrijfsnetwerk is onvoldoende beveiligd tegen cyberinbraken. We hebben kwetsbaarheden ontdekt met een hoge prioriteit. Raadpleeg direct uw IT'er om te onderzoeken of er risico op dataverlies is en om de geconstateerde kwetsbaarheden weg te nemen.

SCORE 5-6 Matig risico

(Actie door uw IT'er nodig)

Uw website of bedrijfsnetwerk is redelijk beveiligd tegen cyberinbraken, maar er zijn kwetsbaarheden gedetecteerd met een gemiddelde prioriteit. Raadpleeg uw IT'er om te onderzoeken of er risico op dataverlies is en om de geconstateerde kwetsbaarheden weg te nemen.

SCORE 7-8 Laag risico

(Actie door uw IT'er gewenst)

Uw website of bedrijfsnetwerk is goed beveiligd tegen cyberinbraken, maar er zijn wel kwetsbaarheden ontdekt. Raadpleeg uw IT'er om te onderzoeken of er risico op dataverlies is en om de geconstateerde kwetsbaarheden weg te nemen.

SCORE 9-10 Erg laag risico

(Geen directe actie nodig, maar laat e.e.a. wel door uw IT'er controleren)

Uw website of bedrijfsnetwerk is zeer goed beveiligd tegen cyberinbraken. Er zijn op dit moment geen of vrijwel geen kwetsbaarheden ontdekt. We adviseren wel om uw IT'er wel naar de geconstateerde kwetsbaarheden te laten kijken.

CVSS score	Mogelijkheid van misbruik bekend (exploit)?	Score ThreadStone	Kwalificatie ThreadStone
Critical	Ja	1	Extreem risico
	Nee	2	
High	Ja	3	Hoog risico
	Nee	4	
Medium	Ja	5	Matig risico
	Nee	6	
Low	Ja	7	Laag risico
	Nee	8	
Information	Ja	9	Erg laag risico
	Nee	10	