VERTROUWELIJK

RAPPORTAGE THREADSCAN

ThreadScan INTERN ONLINE SECURITY

ALGEMENE INFORMATIE

gescand

Scan op: LocalNetwork

Datum scan: 23 januari 2019

ThreadStone CYBER SECURITY

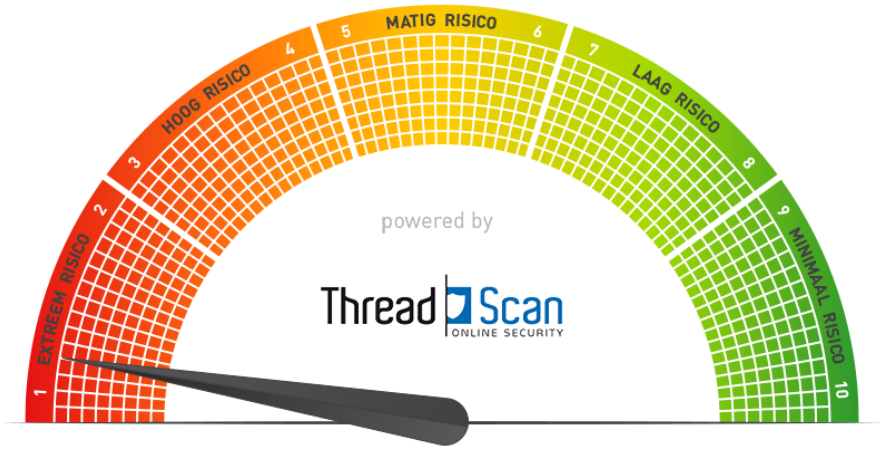
ThreadStone Cyber Security B.V.
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
www.threadstone.eu

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 GLOBALE SCORE VAN DE THREADSCAN IS: 1* (EXTREEM RISICO)

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.

* Gebaseerd op de score-indeling van ThreadStone

Name of host	IP address	Vulnerability score
ubnt	192.168.1.1	1 1 3 1
apple-woonkamer.localdomain	192.168.1.190	1 1
am335x-opt.localdomain	192.168.1.147	1 1 2 1
unifi	192.168.1.3	8 1
LINKSYS00795	192.168.1.2	7 1
iMac	192.168.1.7	1
N/A	192.168.1.40	2 1 4 1
N/A	192.168.1.120	2 1
N/A	192.168.1.41	1 1

Kwetsbaarheden met kritieke prioriteit: 5

Kwetsbaarheden met hoge prioriteit: 3

Kwetsbaarheden met medium prioriteit: 27

Kwetsbaarheden met lage prioriteit: 9

GEVONDEN KWETSBAARHEDEN MET KRITIEKE PRIORITEIT

BESCHRIJVING	CVSS SCORE	Aantal gevonden
OS End Of Life Detection	10,0	1
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10,0	1
LiteServe URL Decoding DoS	9,3	1
libupnp Multiple Buffer Overflow Vulnerabilities	10,0	1
HTTP Brute Force Logins With Default Credentials Reporting	9,0	1

GEVONDEN KWETSBAARHEDEN MET HOGE PRIORITEIT

BESCHRIJVING	CVSS SCORE	Aantal gevonden
TCP timestamps	2,6	1
Generic HTTP Directory Traversal	7,8	1
Report default community names of the SNMP Agent	7,5	1

GEVONDEN KWETSBAARHEDEN MET MEDIUM PRIORITEIT

BESCHRIJVING	CVSS SCORE	Aantal gevonden
Missing `httpOnly` Cookie Attribute	5,0	4
SSH Weak Encryption Algorithms Supported	4,3	2
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4,0	2
SSL/TLS: Report Weak Cipher Suites	4,3	2
PHP Multiple Vulnerabilities - Dec19 (Linux)	6,8	2

SSL/TLS: Missing `secure` Cookie Attribute	6,4	2
HTTP Debugging Methods (TRACE/TRACK) Enabled	5,8	2
Cleartext Transmission of Sensitive Information via HTTP	4,8	3
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5,0	1
libupnp Unhandled POST Write Vulnerability	5,0	1
BrowseGate HTTP headers overflows	5,0	1
Polycom ViaVideo denial of service	5,0	1
mod_access_referer 1.0.2 NULL pointer dereference	5,0	1
Webseal denial of service	5,0	1
FTP Unencrypted Cleartext Login	4,8	1
Keene digital media server XSS	4,3	1

GEVONDEN KWETSBAARHEDEN MET LAGE PRIORITEIT

BESCHRIJVING	CVSS SCORE	Aantal gevonden
SSH Weak MAC Algorithms Supported	2,6	1
TCP timestamps	2,6	8

OS END OF LIFE DETECTION

OMSCHRIJVING

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Found on the ports:

192.168.1.1(general/tcp)

MICROSOFT WINDOWS SMB SERVER NTLM MULTIPLE VULNERABILITIES (971468)

OMSCHRIJVING

This host is missing a critical security update according to
Microsoft Bulletin MS10-012.

Insight

- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.
Impact Level: System/Application

Solution

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx

Found on the ports:

192.168.1.190(445/tcp)

LITESERVE URL DECODING DOS

OMSCHRIJVING

The remote web server dies when an URL consisting of a long invalid string of % is sent.

A cracker may use this flaw to make your server crash continually.

Solution

upgrade your server or firewall it.

Found on the ports:

192.168.1.147(8080/tcp)

LIBUPNP MULTIPLE BUFFER OVERFLOW VULNERABILITIES

OMSCHRIJVING

Updates are available. Please see the references for more information.

Impact

An attacker can exploit these issues to execute arbitrary code in the context of the device that uses the affected library. Failed exploit attempts will likely crash the application.

Solution

libupnp is prone to multiple buffer-overflow vulnerabilities because it fails to perform adequate boundary checks on user-supplied data.

Found on the ports:

192.168.1.40(49153/tcp)

HTTP BRUTE FORCE LOGINS WITH DEFAULT CREDENTIALS REPORTING

OMSCHRIJVING

It was possible to login into the remote Web Application using default credentials.

As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout'
allows you to configure if such an timeout is reported.

Solution

Change the password as soon as possible.

Found on the ports:

192.168.1.40(80/tcp)

TCP TIMESTAMPS

OMSCHRIJVING

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

Found on the ports:

192.168.1.1(general/tcp)

GENERIC HTTP DIRECTORY TRAVERSAL

OMSCHRIJVING

Generic check for HTTP directory traversal vulnerabilities.

Solution

Contact the vendor for a solution.

Found on the ports:

192.168.1.147(8080/tcp)

REPORT DEFAULT COMMUNITY NAMES OF THE SNMP AGENT

OMSCHRIJVING

Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Impact

If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.

If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine.

Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private.

Also note that information made available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

Solution

Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string.

Found on the ports:

192.168.1.40(161/udp)

MISSING `HTTPONLY` COOKIE ATTRIBUTE

OMSCHRIJVING

The application is missing the 'httpOnly' cookie attribute

Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This
allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Solution

Set the 'httpOnly' attribute for any session cookie.

Found on the ports:

192.168.1.1(443/tcp), 192.168.1.3(9090/tcp), 192.168.1.2(443/tcp, 80/tcp)

SSH WEAK ENCRYPTION ALGORITHMS SUPPORTED

OMSCHRIJVING

The remote SSH server is configured to allow weak encryption algorithms.

Insight

The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys.
The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The `none` algorithm specifies that no encryption is to be done.
Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Solution

Disable the weak encryption algorithms.

Found on the ports:

192.168.1.1(22/tcp), 192.168.1.3(22/tcp)

SSL/TLS: DIFFIE-HELLMAN KEY EXCHANGE INSUFFICIENT DH GROUP STRENGTH VULNERABILITY

OMSCHRIJVING

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:
Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Found on the ports:

192.168.1.1(443/tcp), 192.168.1.2(443/tcp)

SSL/TLS: REPORT WEAK CIPHER SUITES

OMSCHRIJVING

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).

- 1024 bit RSA authentication is considered to be insecure and therefore as weak.

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

Solution

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Found on the ports:

192.168.1.147(10001/tcp, 8009/tcp)

PHP MULTIPLE VULNERABILITIES - DEC19 (LINUX)

OMSCHRIJVING

This host is installed with PHP and is prone
to multiple security vulnerabilities.

Insight

The flaws exist due to,

- the imap_open functions which allows to run arbitrary shell commands via mailbox parameter.

- a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile.

Impact

Successful exploitation will allow remote
attackers to execute remote code on affected application/system.

Solution

Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Found on the ports:

192.168.1.3(443/tcp, 80/tcp)

SSL/TLS: MISSING `SECURE` COOKIE ATTRIBUTE

OMSCHRIJVING

The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Insight

The flaw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Solution

Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Found on the ports:

192.168.1.3(9090/tcp), 192.168.1.2(443/tcp)

HTTP DEBUGGING METHODS (TRACE/TRACK) ENABLED

OMSCHRIJVING

Debugging functions are enabled on the remote web server.

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Insight

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Impact

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Disable the TRACE and TRACK methods in your web server configuration.

Please see the manual of your web server or the references for more information.

Found on the ports:

192.168.1.3(443/tcp, 80/tcp)

CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATION VIA HTTP

OMSCHRIJVING

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Found on the ports:

192.168.1.3(9080/tcp), 192.168.1.40(80/tcp), 192.168.1.41(80/tcp)

SSL/TLS: REPORT VULNERABLE CIPHER SUITES FOR HTTPS

OMSCHRIJVING

This routine reports all SSL/TLS cipher suites accepted by a service
where attack vectors exists only on HTTPS services.

Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Solution

The configuration of this services should be changed so
that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Found on the ports:

192.168.1.2(443/tcp)

LIBUPNP UNHANDLED POST WRITE VULNERABILITY

OMSCHRIJVING

libupnp is prone to a unhandled POST write vulnerability

Insight

If there's no registered handler for a POST request, the default
behaviour is to write it to the filesystem. Therefore it is possible to write arbitrary files to it.

Impact

An unauthenticated attacker may write arbitrary files to the filesystem.

Solution

Upgrade to version 1.6.21 or later.

Found on the ports:

192.168.1.2(49153/tcp)

BROWSEGATE HTTP HEADERS OVERFLOWS

OMSCHRIJVING

It was possible to kill the BrowseGate
proxy by sending it an invalid request with too long HTTP headers
(Authorization and Referer)

A cracker may exploit this vulnerability to make your web server
crash continually or even execute arbirtray code on your system.

Solution

upgrade your software or protect it with a filtering reverse proxy

Found on the ports:

192.168.1.2(443/tcp)

POLYCOM VIAVIDEO DENIAL OF SERVICE

OMSCHRIJVING

The remote web server locks up when several incomplete web requests are sent and the connections are kept open.

Insight

Some servers (e.g. Polycom ViaVideo) even run an endless loop, using much CPU on the machine. OpenVAS has no way to test this, but you'd better check your machine.

Solution

Contact your vendor for a patch
Upgrade your web server

Found on the ports:

192.168.1.120(80/tcp)

MOD_ACCESS_REFERER 1.0.2 NULL POINTER DEREFERENCE

OMSCHRIJVING

The remote web server may be using a mod_access_referer apache module which contains a NULL pointer dereference bug.

Impact

Abuse of this vulnerability can possibly be used in denial of service attackers against affected systems.

Solution

Try another access control module, mod_access_referer has not been updated for a long time.

Found on the ports:

192.168.1.40(80/tcp)

WEBSEAL DENIAL OF SERVICE

OMSCHRIJVING

The remote web server dies when an URL ending with %2E is requested.

A cracker may use this flaw to make your server crash continually.

Solution

upgrade your server or firewall it.

Found on the ports:

192.168.1.40(80/tcp)

FTP UNENCRYPTED CLEARTEXT LOGIN

OMSCHRIJVING

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Found on the ports:

192.168.1.40(21/tcp)

KEENE DIGITAL MEDIA SERVER XSS

OMSCHRIJVING

The remote host runs Keene digital media server, a webserver used to share digital information.

This version is vulnerable to multiple cross-site scripting attacks which may allow an attacker to steal the cookies of users of this site.

Solution

Upgrade to the latest version of this software

Found on the ports:

192.168.1.120(80/tcp)

SSH WEAK MAC ALGORITHMS SUPPORTED

OMSCHRIJVING

The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Solution

Disable the weak MAC algorithms.

Found on the ports:

192.168.1.1(22/tcp)

TCP TIMESTAMPS

OMSCHRIJVING

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

Found on the ports:

192.168.1.190(general/tcp), 192.168.1.147(general/tcp), 192.168.1.3(general/tcp), 192.168.1.2(general/tcp), 192.168.1.7(general/tcp), 192.168.1.120(general/tcp), 192.168.1.40(general/tcp), 192.168.1.41(general/tcp)

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	