# SecPoint Nederland - Volledige Rapport

## Scan Naam: Jouw bedrijf

## Uitgevoerd op 2018-05-17 21:46:24

**Vertrouwelijk**

# Inhoudsopgave

**Introductie** ..... 3
**Kwetsbaarheidsniveaus** ..... 4
**Managementsamenvatting** ..... 5
**Traceroute** ..... 7
**Besturingssystemen** ..... 8
**Geïdentificeerde poorten en diensten** ..... 9
**Versie Banner geïdentificeerd** ..... 10
**Samenvatting van de gedetecteerde kwetsbaarheden** ..... 11
**Kwetsbaarheden** ..... 13
Doelsysteem: Jouw bedrijf ..... 13

# Introductie

Dit rapport is het resultaat van een "online kwetsbaarheid beoordelingsscan", uitgevoerd door **SecPoint Nederland**.

Het doel van dit document is om een rapport aan te bieden, waarmee het beveiligniveau van computersystemen en/of IT-apparatuur, aangesloten op het internet, verhoogd wordt.

De kwetsbaarheden worden gecategoriseerd onder één van de vier categorieën: 1.Hoog risico, 2.Gemiddeld risico, 3.Laag risico of 4.Informatief.Een gedetailleerde uitleg van elke kwetsbaarheidscategorie kan worden gevonden onder de alinea **Beveiligingsniveaus**.

Deze **samenvatting** is speciaal samengesteld voor een beheer niveau beoordeling. Deze samenvatting bevat zowel geschreven als grafische informatie op basis van de resultaten van de scanner. Deze resultaten omvatten dergelijke informatie zoals; wanneer de scan werd uitgevoerd; wie de scan uitgevoerd heeft en hoeveel systeem kwetsbaarheden gevonden werden in elke categorie.

De **samenvatting** bevat ook een concluderende rapportage van het algemene beveiligingsniveau van het geteste systeem.

Details en namen van kwetsbaarheden die ontdekt zijn, zijn te vinden onder het kopje; **overzicht van kwetsbaarheden**. Dit wordt vervolgd door de individuele beschrijvingen van de vaststelling van elke gevonden kwetsbaarheid.

Waar mogelijk, een Bugtraq ID, een CVE **en/of** een USN aanwezig zijn. voor meer informatie.

Elk systeem zijn kwetsbaarheid ontdekt wordt geleverd met een mogelijke oplossing.

**(*) Bugtraq ID is de officiële Securityfocus.com ID; Ook bekend als bugtraq.**
**(**) CVE is de officiële CVE Mitre lijst.**
**(***) USN is de officiële Ubuntu Beveiliging kennisgeving lijst.**

# Kwetsbaarheidsniveaus

## Hoge Risico beveiligingslekken

Wanneer een hoge risico kwetsbaarheid geïdentificeerd wordt, betekent dat het mogelijk is voor een indringer uw netwerk binnen te treden, het systeem volledig beheren en / of toegang tot zeer gevoelige systeeminformatie te verkrijgen. Dit op zijn beurt kan leiden tot diefstal of verlies van privé en gevoelige gegevens.

## Gemiddelde Risico beveiligingslekken

Wanneer een gemiddelde kwetsbaarheid risico wordt vastgesteld, betekent dit dat een indringer toegang tot het systeem heeft. De indringer kan informatie bereiken wat kan leiden tot meer specifieke aanvallen en eventueel een volledig systeem compromis kan bereiken. Dit op zijn beurt kan leiden tot diefstal of verlies van privé en gevoelige gegevens.

## Lage Risico beveiligingslekken

Wanneer een lage kwetsbaarheid risico wordt vastgesteld, betekent dit meestal dat een indringer toegang tot de systeem informatie heeft, wat kan leiden tot meer specifieke aanvallen en uiteindelijk resulteert in de diefstal of verlies van persoonlijke en privé gegevens.

## Informatie

Alle inzendingen op dit niveau bieden aanvullende informatie die al beschikbaar is over het geteste systeem. Het geeft niet aan of het systeem wel of niet kwetsbaar is.

# Managementsamenvatting

Dit verslag is een beveiligingsscan uitgevoerd door **SecPoint Nederland**. Dit rapport bevat betrouwbare informatie over de toestand van uw netwerk/systeem. De toegang tot deze informatie door onbevoegd personeel kan hen in staat stellen om uw netwerkbeveiliging in gevaar te brengen.

| | | | |
|---|---|---|---|
| **Scan Naam** | jouwbedrijf.nl | **Scanprofiel** | SSL CMS Scan |
| **Gestart op** | 2018-05-17 21:46:24 | **Eindigde op** | 2018-05-18 08:53:57 |
| **Duur** | 11:07:33 (11 hours, 7 minutes, 33 seconds) | | |
| **Scan Engine** | 9.9.1.297 | | |
| **Gecontroleerde Doelsysteem** | jouwbedrijf.nl | | |

Deze scan is uitgevoerd met door gebruiker **Test**

## Algemeen beveiligingsniveau

**Cat. 1 (Kritiek niveau)**

De scan uitgevoerd door **SecPoint Nederland** heeft het volgende vastgesteld: Het beveiligingsniveau van uw systeem: - Is gevaarlijk laag. Het is mogelijk voor indringers dit systeem volledig over te nemen, dit kan resulteren in verlies van persoonlijke en gevoelige informatie. Het wordt aanbevolen dat u onmiddellijk actie onderneemt om het beveiligingsniveau te verbeteren.

## Online Nodes

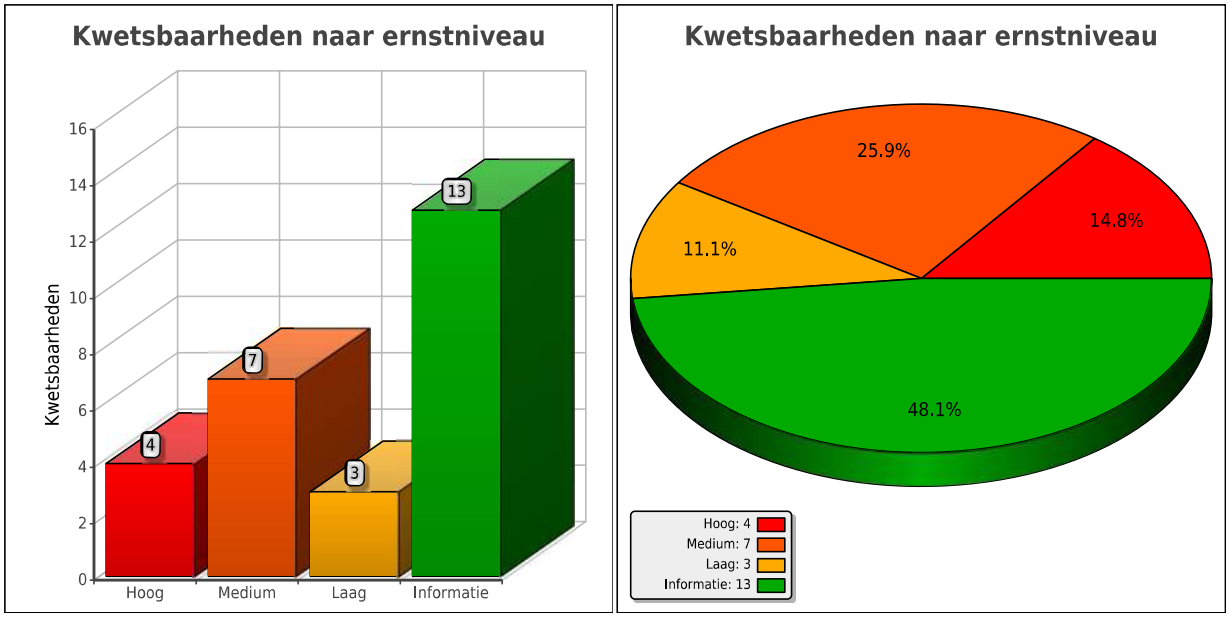
Alle knooppunten waren online bij de scan.

## Offline Nodes

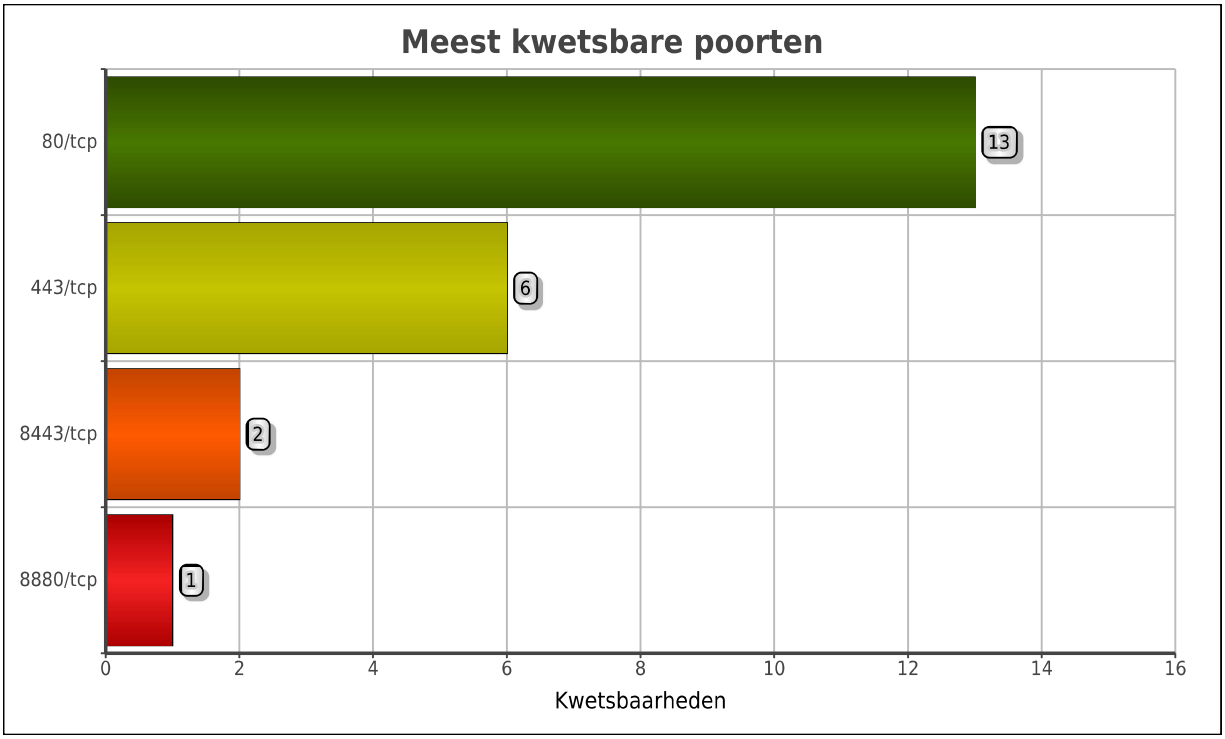
De scan is niet gedetecteerd geen offline knooppunten.

## Analyse van Resultaten

Een totaal van **27** potentiële kwetsbaarheden werd geïdentificeerd op de doelsystemen, met een ratio van **14.8%** van kwetsbaarheden op hoog niveau.




*Totaal aantal kwetsbaarheden*




*Lijst met de meest kwetsbare poorten, op basis van het aantal kwetsbaarheden dat op die poort is aangetroffen*

# Traceroute

Dit is het resultaat van een traceroute van SecPoint Nederland naar de doelsystemen:

**traceroute to , 15 hops max, 60 byte packets**

| Hop | Naam | IP | Plaats | Gem (ms) | Diagram |
|---|---|---|---|---|---|
| 1 | | | Netherlands | 0.614 | |
| 2 | | | Netherlands | 14.426 | |
| 3 | | | - | - | - |
| 4 | | | Netherlands | 15.572 | |
| 5 | | | Germany(16) Berlin | 26.226 | |
| 6 | | | Germany(16) Berlin | 25.836 | |
| 7 | | | - | - | - |
| 8 | | | Germany(16) Berlin | 25.349 | |

# Besturingssystemen

De volgende besturingssystemen zijn geïdentificeerd:

**Doelsysteem: jouwbedrijf.nl**

Linux 3.x

# Geïdentificeerde poorten en diensten

De volgende poorten en diensten werden geïdentificeerd op de doelsystemen:

**Poorten en diensten voor: Jouwbedrijf.nl**

| Poort | Protocol | Status | Service |
|---|---|---|---|
| 80 | tcp | open | World Wide Web HTTP |
| 443 | tcp | open | http protocol over TLS/SSL |
| 8443 | tcp | open | PCsync HTTPS |
| 8880 | tcp | open | CDDBP |

# Versie Banner geïdentificeerd

De volgende Dienst Uitvoering Banner uitgangen waren leesbaar op de doelsystemen.
Het wordt sterk aangeraden om deze banners met geen of nep informatie compleet te her configureren.

### Dienst Uitvoering Banners voor: jouwbedrijf.nl

| | |
|---|---|
| **Banner Naam** | HTTP Version Banner |
| **Poort** | 80/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

| | |
|---|---|
| **Banner Naam** | HTTP Version Banner |
| **Poort** | 443/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

| | |
|---|---|
| **Banner Naam** | HTTP Version Banner |
| **Poort** | 8443/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

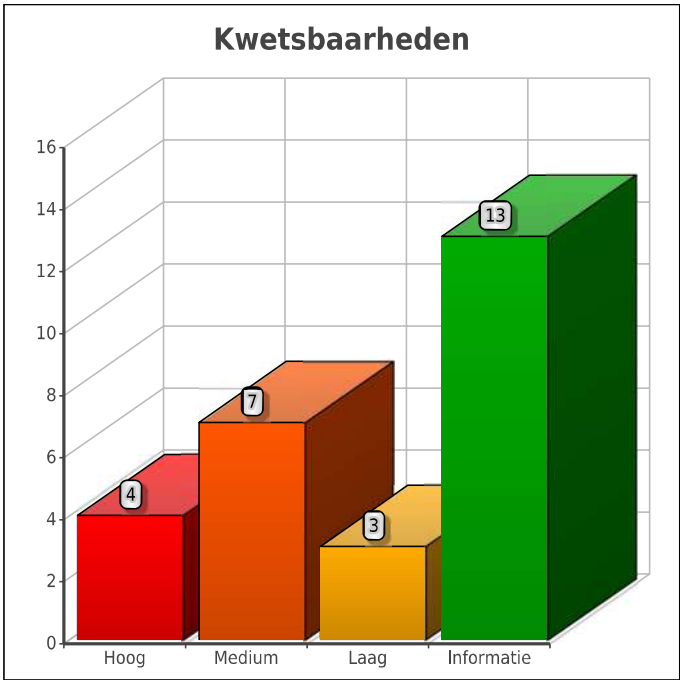
| | |
|---|---|
| **Banner Naam** | HTTP Version Banner |
| **Poort** | 8880/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

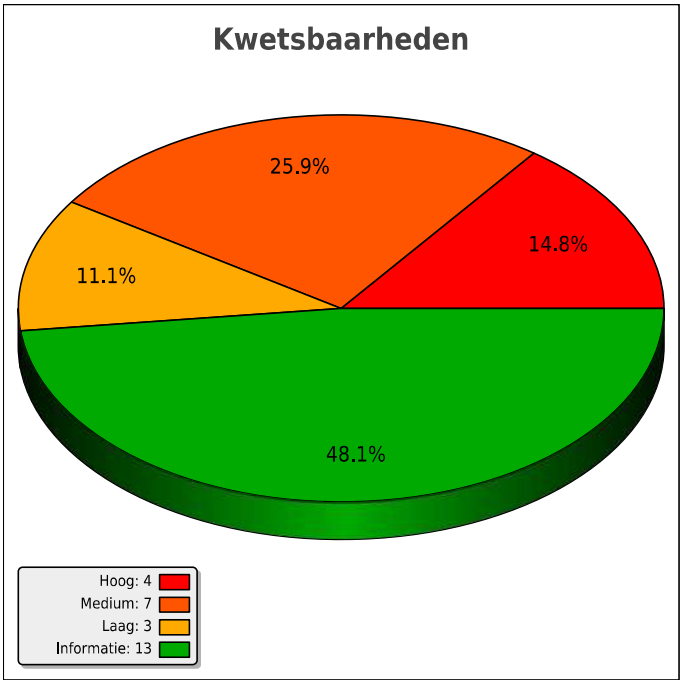
| | |
|---|---|
| **Banner Naam** | HTTPS Version Banner |
| **Poort** | 443/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

| | |
|---|---|
| **Banner Naam** | HTTPS Version Banner |
| **Poort** | 8443/tcp |
| **Details** | Apache |
| **Oplossing** | It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. |

# Samenvatting van de gedetecteerde kwetsbaarheden

### Doelsysteem: jouwbedrijf.nl




| Risico niveau | Kwetsbaarheid |
|---|---|
| | HTTP only port without SSL found |
| | File general-template.php File Inclusion |
| | File pluggable.php File Inclusion |
| | File web.config accessible on remote web server |
| | File admin-footer.php Information Disclosure |
| | File moderation.php Information Disclosure |
| | File edit-link-form.php Information Disclosure |
| | File edit-form-comment.php Information Disclosure |
| | license.txt File Information Disclosure |
| | File edit-form-advanced.php Information Disclosure |
| | Target SSL Beast Vulnerability Check |
| | Default Apache README File Information Disclosure |
| | SSL Vulnerability LUCKY13 Vulnerability |
| | Self Issued SSL Cert [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590) |
| | Web Speedtest Fast 1 Seconds lag Port: 443 |
| | Web Speedtest Fast 0 Seconds lag Port: 8443 |
| | All Protocols Tested |
| | Web Speedtest Slow 5 Seconds lag Port: 80 |
| | System Time Revealed via. ICMP TimeStamp |
| | Identified Operating System Linux 3.x Packet Check #3 |

| Risico niveau | Kwetsbaarheid |
|---|---|
| | SSL Certificate information |
| | Apache Identified |
| | WordPress Version Identified |
| | WordPress Theme Identified |
| | System time via remote Web Server |
| | Remote system answers to PING command |
| | Web Speedtest Fast 0 Seconds lag Port: 8880 |

# Kwetsbaarheden

### Doelsysteem: jouwbedrijf.nl

| Kwetsbaarheid | HTTP only port without SSL found |
|---|---|
| Risico niveau | Hoog |
| Poort | 80/tcp |
| SecPoint ID | 58373 |
| Invloed | The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information. The service is also running on 8880/tcp. |
| Oplossing | It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. |
| Uitgang gevoeligheid/Bewijzen. | |
| | AttackOutput: Protocol on tcp matches http |

| Kwetsbaarheid | File general-template.php File Inclusion |
|---|---|
| Risico niveau | Hoog |
| Poort | 80/tcp |
| SecPoint ID | 9984 |
| Invloed | The identified file found on the remote web server is subject to a remote file inclusion vulnerability. An attacker can exploit this vulnerability to include remote files and execute arbitrary code on the target system. |
| Oplossing | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| Uitgang gevoeligheid/Bewijzen. | |
| | AttackString: GET http://<br><br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:19:39 GMT<br>Server: Apache<br>X-Powered-By: PleskLin<br>Cache-Control: max-age=0, no-cache, s-maxage=10<br>Content-Length: 0<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8 |

| Kwetsbaarheid | File pluggable.php File Inclusion |
|---|---|
| Risico niveau | Hoog |
| Poort | 80/tcp |
| SecPoint ID | 10307 |

| | |
|---|---|
| **Invloed** | The identified file found on the remote web server is subject to a remote file inclusion vulnerability. An attacker can exploit this vulnerability to include remote files and execute arbitrary code on the target system. |
| **Oplossing** | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:18:25 GMT<br>Server: Apache<br>X-Powered-By: PleskLin<br>Cache-Control: max-age=0, no-cache, s-maxage=10<br>Content-Length: 0<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8 |

| **Kwetsbaarheid** | **File web.config accessible on remote web server** |
|---|---|
| **Risico niveau** | Hoog |
| **Poort** | 80/tcp |
| **SecPoint ID** | 4047 |
| **Invloed** | The identified jserv.conf file found on the remote web server was found accessible. This file is known to contain sensitive information on the target system. |
| **Oplossing** | It is recommended to upgrade to the latest version of the software you are running on the web interface and or set permissions so the the jserv.conf file is not accessible. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:59:38 GMT<br>Server: Apache<br>Last-Modified: Wed, 16 May 2018 11:04:48 GMT<br>ETag: "a6-56c50afee74f9"<br>Accept-Ranges: bytes<br>Content-Length: 166<br>X-Powered-By: PleskLin<br>Cache-Control: s-maxage=10<br>Connection: close<br><?xml version="1.0" encoding="UTF-8"?><br><!-- Reset by Duplicator Installer. Original can be found in web.config.180516110448.orig --><br><configuration></configuration> |

| **Kwetsbaarheid** | **File admin-footer.php Information Disclosure** |
|---|---|
| **Risico niveau** | Medium |

| | |
|---|---|
| **Poort** | 80/tcp |
| **SecPoint ID** | 13284 |
| **Invloed** | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| **Oplossing** | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:44:17 GMT<br>Server: Apache<br>Vary: Accept-Encoding<br>X-Powered-By: PleskLin<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8<br>-1 |

| | |
|---|---|
| **Kwetsbaarheid** | **File moderation.php Information Disclosure** |
| **Risico niveau** | Medium |
| **Poort** | 80/tcp |
| **SecPoint ID** | 13264 |
| **Invloed** | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| **Oplossing** | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 302 Found<br>Date: Fri, 18 May 2018 07:44:09 GMT<br>Server: Apache<br>Set-Cookie: wfvt_1361933426=5afe84499050b<br>expires=Fri, 18-May-2018 08:14:09 GMT<br>Max-Age=1800<br>path=/<br>HttpOnly<br>Location:<br>http://<br>X-Powered-By: PleskLin<br>Content-Length: 0<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8 |

| Kwetsbaarheid | File edit-link-form.php Information Disclosure |
|---|---|
| Risico niveau | Medium |
| Poort | 80/tcp |
| SecPoint ID | 13289 |
| Invloed | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| Oplossing | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| Uitgang gevoeligheid/Bewijzen. | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:44:18 GMT<br>Server: Apache<br>Vary: Accept-Encoding<br>X-Powered-By: PleskLin<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8<br>-1 |

| Kwetsbaarheid | File edit-form-comment.php Information Disclosure |
|---|---|
| Risico niveau | Medium |
| Poort | 80/tcp |
| SecPoint ID | 13288 |
| Invloed | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| Oplossing | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| Uitgang gevoeligheid/Bewijzen. | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:44:18 GMT<br>Server: Apache<br>Vary: Accept-Encoding<br>X-Powered-By: PleskLin<br>Connection: close<br>Content-Type: text/html<br>charset=UTF-8<br>-1 |

| Kwetsbaarheid | license.txt File Information Disclosure |
|---|---|
| Risico niveau | Medium |
| Poort | 80/tcp |

| | |
|---|---|
| **SecPoint ID** | 56006 |
| **Invloed** | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| **Oplossing** | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http://<br>AttackOutput: HTTP/1.1 200 OK<br>Date: Fri, 18 May 2018 07:37:16 GMT<br>Server: Apache<br>Last-Modified: Wed, 16 May 2018 11:04:30 GMT<br>ETag: "4ddf-56c50aedce91b"<br>Accept-Ranges: bytes<br>Content-Length: 19935<br>Vary: Accept-Encoding<br>X-Powered-By: PleskLin<br>Cache-Control: s-maxage=10<br>Connection: close<br>Content-Type: text/plain<br>WordPress - Web publishing software<br>Copyright 2011-2018 by the contributors<br>This program is free software<br>you can redistribute it and/or modify<br>it under the terms of the GNU General Public License as published by<br>the Free Software Foundation<br>either version 2 of the License, or<br>(at your option) any later version.<br>This program is distributed in the hope that it will be useful,<br>but WITHOUT ANY WARRANTY<br>without even the implied warranty of<br>MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the<br>GNU General Public License for more details.<br>You should have received a copy of the GNU General Public License<br>along with this program<br>if not, write to the Free Software<br>Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA<br>This program incorporates work covered by the following copyright and<br>permission notices:<br>b2 is (c) 2001, 2002 Michel Valdrighi - m@tidakada.com -<br>http://tidakada.com<br>Wherever third party code has been used, credit has been given in the codes<br>comments.<br>b2 is released under the GPL<br>and<br>WordPress - Web publishing software<br>Copyright 2003-2010 by the contributors<br>WordPress is released under the GPL |

| | |
|---|---|
| | =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-= |
| | GNU GENERAL PUBLIC LICENSE |
| | Version 2, June 1991 |
| | Copyright (C) 1989, 1991 Free Software Foundation, Inc., |
| | 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA |
| | Everyone is permitted to copy and distribute verbatim copies |
| | of this license document, but changing it is not allowed. |
| | Preamble |
| | The licenses for most software are designed to take away |

| **Kwetsbaarheid** | **File edit-form-advanced.php Information Disclosure** |
|---|---|
| **Risico niveau** | Medium |
| **Poort** | 80/tcp |
| **SecPoint ID** | 13287 |
| **Invloed** | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| **Oplossing** | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackString: GET http:// |
| | AttackOutput: HTTP/1.1 200 OK |
| | Date: Fri, 18 May 2018 07:44:18 GMT |
| | Server: Apache |
| | Vary: Accept-Encoding |
| | X-Powered-By: PleskLin |
| | Connection: close |
| | Content-Type: text/html |
| | charset=UTF-8 |
| | -1 |

| **Kwetsbaarheid** | **Target SSL Beast Vulnerability Check** |
|---|---|
| **Risico niveau** | Medium |
| **Poort** | 443/tcp |
| **SecPoint ID** | 58279 |
| **CVE** | CVE-2011-3389 |
| **USN** | 1263-1 |
| **Invloed** | The SSL Protocol used in Microsoft Windows and popoular browsers such as Firefox, Google Chrome, Operate are using a CBC mode with chained initialization vectors which are vulnerable to Man in the Middel Attacks. Please note this attack is only client site. The service is also running on 8443/tcp. |
| **Oplossing** | It is recommended to update your operating system to the latest packages or upgrade to the latest openssl from http://www.openssl.org/ |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | AttackOutput: VULNERABLE -- but also supports higher protocols (possible mitigation): TLSv1.1 TLSv1.2 |

| Kwetsbaarheid | Default Apache README File Information Disclosure |
|---|---|
| Risico niveau | Laag |
| Poort | 80/tcp |
| SecPoint ID | 55991 |
| Invloed | The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. |
| Oplossing | Please upgrade to the latest version of the identified software you are running with the found file. NOTE: If you are already running the latest version please ignore this check. |
| Uitgang gevoeligheid/Bewijzen. | |
| | AttackString: GET http:// |
| | AttackOutput: HTTP/1.1 200 OK |
| | Date: Fri, 18 May 2018 07:37:15 GMT |
| | Server: Apache |
| | Last-Modified: Tue, 28 Aug 2007 10:47:54 GMT |
| | ETag: "13f4-438c034968a80" |
| | Accept-Ranges: bytes |
| | Content-Length: 5108 |
| | X-Powered-By: PleskLin |
| | Cache-Control: s-maxage=10 |
| | Connection: close |
| | Public Domain Icons |
| | These icons were originally made for Mosaic for X and have been |
| | included in the NCSA httpd and Apache server distributions in the |
| | past. They are in the public domain and may be freely included in any |
| | application. The originals were done by Kevin Hughes (kevinh@kevcom.com). |
| | Andy Polyakov tuned the icon colors and added a few new images. |
| | If youd like to contribute additions to this set, contact the httpd |
| | documentation project <http://httpd.apache.org/docs-project/>. |
| | Almost all of these icons are 20x22 pixels in size. There are |
| | alternative icons in the "small" directory that are 16x16 in size, |
| | provided by Mike Brown (mike@hyperreal.org). |
| | Suggested Uses |
| | The following are a few suggestions, to serve as a starting point for ideas. |
| | Please feel free to tweak and rename the icons as you like. |
| | a.gif |
| | This might be used to represent PostScript or text layout |
| | languages. |
| | alert.black.gif, alert.red.gif |
| | These can be used to highlight any important items, such as a |
| | README file in a directory. |
| | back.gif, forward.gif |
| | These can be used as links to go to previous and next areas. |
| | ball.gray.gif, ball.red.gif |
| | These might be used as bullets. |

| | |
|---|---|
| | binary.gif<br>This can be used to represent binary files.<br>binhex.gif<br>This can represent BinHex-encoded data.<br>blank.gif<br>This can be used as a placeholder or a spacing element.<br>bomb.gif<br>This can be used to represent core files.<br>box1.gif, box2.gif<br>These icons can be used to represent generic 3D applications and related files.<br>broken.gif<br>This can represent corrupted data.<br>burst.gif |

| Kwetsbaarheid | SSL Vulnerability LUCKY13 Vulnerability |
|---|---|
| Risico niveau | Laag |
| Poort | 443/tcp |
| SecPoint ID | 58281 |
| CVE | CVE-2013-0169 |
| USN | 1732-3 |
| USN | 1735-1 |
| USN | 1732-1 |
| Invloed | The TLS Protocol 1.1, 1.2 & DTLS protocol 1.0, 1.2 which are used in OpenSSL OpenJDK PolarSSL do not prevent timing side channel attacks on a MAC check. This allows remote attackers to conduct distinguishing attacks and plaintext recovery attacks. Timing data for crafted packets aka Lucky Thirteen. The service is also running on 8443/tcp. |
| Oplossing | It is recommended to disable SSLv3 by opening httpd.conf and adding: SSLProtocol All -SSLv2 -SSlv3 |
| Uitgang gevoeligheid/Bewijzen. | |
| | LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS |

| Kwetsbaarheid | Self Issued SSL Cert [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590) |
|---|---|
| Risico niveau | Laag |
| Poort | 443/tcp |
| SecPoint ID | 56214 |
| Invloed | Self-issued certificates can't ensure connection details; visitors of the site can't be sure if it is not a fake site/certificate |
| Oplossing | Consider upgrading your certificate or buying it from well-known issuer |
| Uitgang gevoeligheid/Bewijzen. | |
| | [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590) |

| Kwetsbaarheid | Web Speedtest Fast 1 Seconds lag Port: 443 |
|---|---|

| | |
|---|---|
| **Risico niveau** | Informatie |
| **Poort** | 443/tcp |
| **SecPoint ID** | 58 |
| **Invloed** | The target Web server speed was determined. |
| **Oplossing** | If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Penetrator. It is recommended to white list the Penetrator for the best result. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | 1 |

| **Kwetsbaarheid** | **Web Speedtest Fast 0 Seconds lag Port: 8443** |
|---|---|
| **Risico niveau** | Informatie |
| **Poort** | 8443/tcp |
| **SecPoint ID** | 58 |
| **Invloed** | The target Web server speed was determined. |
| **Oplossing** | If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Penetrator. It is recommended to white list the Penetrator for the best result. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | 0 |

| **Kwetsbaarheid** | **All Protocols Tested** |
|---|---|
| **Risico niveau** | Informatie |
| **SecPoint ID** | 8311 |
| **Invloed** | This check probes all ports for their real protocols. If all matches as it should be please ignore this check. |
| **Oplossing** | If there is found known services on unknown ports it is recommended to properly test those ports. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | Protocol on /tcp matches http |
| | Protocol on /tcp matches http-proxy |
| | Protocol on /tcp matches http |
| | Protocol on /tcp matches http-proxy |
| | Protocol on /tcp matches ssl |
| | Protocol on /tcp matches http |
| | Protocol on /tcp matches ssl |
| | Protocol on /tcp matches http |

| **Kwetsbaarheid** | **Web Speedtest Slow 5 Seconds lag Port: 80** |
|---|---|
| **Risico niveau** | Informatie |
| **Poort** | 80/tcp |
| **SecPoint ID** | 58 |
| **Invloed** | The target Web server speed was determined. |
| **Oplossing** | If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Penetrator. It is recommended to white list the Penetrator for the best result. |

| Uitgang gevoeligheid/Bewijzen. | |
|---|---|
| | 5 |

| Kwetsbaarheid | System Time Revealed via. ICMP TimeStamp |
|---|---|
| Risico niveau | Informatie |
| SecPoint ID | 1746 |
| CVE | CVE-1999-0524 |
| Invloed | By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 22:48:13. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests. |
| Oplossing | At network-level this traffic should be rejected both inbound and outbound.<br>UNIX:<br>ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly.<br>WINDOWS:<br>This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.On a Cisco device it can be blocked by setting the rules<br>access-list 101 deny icmp any any 13 ! timestamp request. |

| Kwetsbaarheid | Identified Operating System Linux 3.x Packet Check #3 |
|---|---|
| Risico niveau | Informatie |
| Poort | 8443/tcp |
| SecPoint ID | 58 |
| Invloed | Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operaitng system is end of life and wide open to attacks and wont be patched. |
| Oplossing | It is recommended to clean the identified version banner so it reveals as less information as possible. |
| Uitgang gevoeligheid/Bewijzen. | |
| | `Linux 3.x` |

| Kwetsbaarheid | SSL Certificate information |
|---|---|
| Risico niveau | Informatie |
| Poort | 443/tcp |
| SecPoint ID | 3702 |
| Invloed | It is possible to retrieve the SSL certificate owner information from the target web server running. In this check please review the vulnerability information provided from the ssl certificate. The service is also running on 8443/tcp. |
| Oplossing | If all the information in the certificate output is the correct information and matches what it is supposed to please ignore this check. |
| Uitgang gevoeligheid/Bewijzen. | |
| | `subject=/C=CH/L=Schaffhausen/O=Plesk/CN=Plesk/emailAddress=info@plesk.com`<br>`issuer=/C=CH/L=Schaffhausen/O=Plesk/CN=Plesk/emailAddress=info@plesk.com` |

| Kwetsbaarheid | Apache Identified |
|---|---|
| Risico niveau | Informatie |
| Poort | 443/tcp |
| SecPoint ID | 2436 |
| Invloed | It is possible via the banner from the web server software to detect some presence of Apache. Apache has a known history of several security vulnerabilities. Attackers can use this information to do Apache specified attacks. The service is also running on 80/tcp, 443/tcp. |
| Oplossing | To reconfigure the apache banner. 1: First make backup of all files we will modify<br>2: From the apache source package find the following file /apache/src/include/httpd.h and open it up in an editor.<br>3: Find the following fields: SERVER_BASEVENDOR SERVER_BASEPRODUCT SERVER_BASEVERSION and reset all values in them so that it looks like<br>SERVER_BASEVENDOR ""<br>SERVER_BASEPRODUCT ""<br>SERVER_BASEVERSION "". |
| Uitgang gevoeligheid/Bewijzen. | |
| | Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0 |
| | AttackOutput: HTTP/1.1 200 OK |
| | Date: Fri, 18 May 2018 06:08:45 GMT |
| | Server: Apache |
| | Accept-Ranges: bytes |
| | Vary: Accept-Encoding |
| | X-Mod-Pagespeed: 1.13.35.2-0 |
| | X-Powered-By: PleskLin |
| | MS-Author-Via: DAV |
| | Cache-Control: max-age=0, no-cache |
| | Content-Length: 5491 |
| | Connection: close |
| | Content-Type: text/html |

| Kwetsbaarheid | WordPress Version Identified |
|---|---|
| Risico niveau | Informatie |
| SecPoint ID | 49151 |
| Invloed | The identified WordPress found running is showing the version of the installed Wordpress. An attacker can use this information to base other attacks on. They can search for the theme and match for vulnerabilities. |
| Oplossing | If possible change the identified in the WordPress version. |
| Uitgang gevoeligheid/Bewijzen. | |
| | [32m[+][0m WordPress version 4.9.5 identified from meta generator (Released on 2018-04-03) |

| Kwetsbaarheid | WordPress Theme Identified |
|---|---|

| | |
|---|---|
| **Risico niveau** | Informatie |
| **SecPoint ID** | 49150 |
| **Invloed** | The identified WordPress found running is showing the name of the installed Theme. An attacker can use this information to base other attacks on. They can search for the theme and match for vulnerabilities. |
| **Oplossing** | If possible change the name identified in the WordPress theme. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | `[32m[+][0m WordPress theme in use:` |

| **Kwetsbaarheid** | **System time via remote Web Server** |
|---|---|
| **Risico niveau** | Informatie |
| **Poort** | 80/tcp |
| **SecPoint ID** | 1745 |
| **Invloed** | It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests. The service is also running on 443/tcp, 8443/tcp, 8880/tcp. |
| **Oplossing** | Since this is a default option in most web servers, it has to be reconfigured without the Date function.<br>Apache:<br>It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time))<br>and UN Comment the line by setting a // in-front of the line.<br>After that find the line ap_table_unset(r->headers_out, "Date")<br>and put a // in-front of that line as well. Now recompile apache.<br>IIS<br>This is not directly possible here and has to be done on firewall level or by applying thrid party software.<br>IIS WINDOWS<br>This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it. |
| **Uitgang gevoeligheid/Bewijzen.** | |
| | `AttackString: HEAD / HTTP/1.0` |
| | `AttackOutput: Thu, 17 May 2018 21:49:11 GMT` |

| **Kwetsbaarheid** | **Remote system answers to PING command** |
|---|---|
| **Risico niveau** | Informatie |
| **SecPoint ID** | 2853 |
| **Invloed** | The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this. |
| **Oplossing** | It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 . |

| Uitgang gevoeligheid/Bewijzen. | |
|---|---|
| | 64 octets from : icmp_seq=0 ttl=58 time=25.8 ms |

| Kwetsbaarheid | Web Speedtest Fast 0 Seconds lag Port: 8880 |
|---|---|
| Risico niveau | Informatie |
| Poort | 8880/tcp |
| SecPoint ID | 58 |
| Invloed | The target Web server speed was determined. |
| Oplossing | If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Penetrator. It is recommended to white list the Penetrator for the best result. |
| Uitgang gevoeligheid/Bewijzen. | |
| | 0 |