

Reconnaisance Website

Tugas 1 Keamanan Jaringan Komputer



Disusun Oleh :

Nama : Siti Aisyah

NIM : 09011181621024

Jurusan : Sistem Komputer

Dosen : Deris Stiawan, M.T., Ph.D.


Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

1. www.perex.com

Network

- Site : <http://www.perex.com>
- Domain : perex.com
- IP address : 104.236.219.51
- Ipv6 Address : -
- Domain Registrar : google.com
- Organisation : Contact Privacy Inc. Customer 124127711, 96 Mowat Ave,
Toronto, M4K 3K1, Canada
- Top level domain : Commercial entities (.com)
- Hosting country :  [US](#)
- Netblock Owner : [DigitalOcean, LLC](#)
- Nameserver : ns-cloud-e1.googledomains.com
- DNS admin : dns-admin@google.com
- Reverse DNS : perex.com
- Nameserver organisation : whois.markmonitor.com
- Hosting company : DigitalOcean
- DNS Security Extensions :-

Registrar Information

- Domain Name: perex.com
- Registry Domain ID: 85652841_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.google.com
- Registrar URL: <https://domains.google.com>
- Updated Date: 2018-04-17T00:41:42Z
- Creation Date: 2002-04-16T18:32:37Z
- Registrar Registration Expiration Date: 2019-04-16T18:32:37Z
- Registrar: Google LLC

- Registrar IANA ID: 895
- Registrar Abuse Contact Email: registrar-abuse@google.com
- Registrar Abuse Contact Phone: +1.8772376466
- Domain Status: clientTransferProhibited
- <https://www.icann.org/epp#clientTransferProhibited>
- Registry Registrant ID:
- Registrant Name: Contact Privacy Inc. Customer 124127711
- Registrant Organization: Contact Privacy Inc. Customer 124127711
- Registrant Street: 96 Mowat Ave
- Registrant City: Toronto
- Registrant State/Province: ON
- Registrant Postal Code: M4K 3K1
- Registrant Country: CA
- Registrant Phone: +1.4165385487
- Registrant Phone Ext:
- Registrant Fax:
- Registrant Fax Ext:
- Registrant Email: cibendddjd2h@contactprivacy.email
- Registry Admin ID:
- Admin Name: Contact Privacy Inc. Customer 124127711
- Admin Organization: Contact Privacy Inc. Customer 124127711
- Admin Street: 96 Mowat Ave
- Admin City: Toronto
- Admin State/Province: ON
- Admin Postal Code: M4K 3K1
- Admin Country: CA
- Admin Phone: +1.4165385487
- Admin Phone Ext:
- Admin Fax:
- Admin Fax Ext:

- Admin Email: cibendddjd2h@contactprivacy.email
- Registry Tech ID:
- Tech Name: Contact Privacy Inc. Customer 124127711
- Tech Organization: Contact Privacy Inc. Customer 124127711
- Tech Street: 96 Mowat Ave
- Tech City: Toronto
- Tech State/Province: ON
- Tech Postal Code: M4K 3K1
- Tech Country: CA
- Tech Phone: +1.4165385487
- Tech Phone Ext:
- Tech Fax:
- Tech Fax Ext:
- Tech Email: cibendddjd2h@contactprivacy.email
- Name Server: NS-CLOUD-E1.GOOGLEDOMAINS.COM
- Name Server: NS-CLOUD-E2.GOOGLEDOMAINS.COM
- Name Server: NS-CLOUD-E3.GOOGLEDOMAINS.COM
- Name Server: NS-CLOUD-E4.GOOGLEDOMAINS.COM
- DNSSEC: unsigned

Hosting

- DigitalOcean, LLC 101 Ave of the Americas 10th Floor New York NY US 10013
 - IP address : 104.236.219.51
 - OS : Linux
 - Webserver : Apache/2.4.6 CentOS PHP/5.4.16
 - Tanggal : 10-Feb-2019

Site Technology

- Application Servers : CentOS, Apache
- Server-Side : PHP, PHP Enabled
- Character Encoding : UTF8
- Doctype : HTML
- CSS Usage : Embedded

CVE

[Apache](#) » [Http Server](#) » **2.4.6 : Security Vulnerabilities (Denial Of Service)**

Cpe Name: [cpe:/a:apache:http_server:2.4.6](#)
 CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)
 Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)
[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15710	787		DoS	2018-03-26	2018-11-13	5.0	None	Remote	Low	Not required	None	None	Partial
<p>In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.</p>														
2	CVE-2017-9788	20		DoS +Info	2017-07-13	2018-01-04	6.4	None	Remote	Low	Not required	Partial	None	Partial
<p>In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.</p>														
3	CVE-2014-3523	399		DoS	2014-07-20	2018-01-04	5.0	None	Remote	Low	Not required	None	None	Partial
<p>Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.</p>														
4	CVE-2014-0231	399		DoS	2014-07-20	2018-10-30	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.</p>														
5	CVE-2014-0226	362	1	DoS Exec Code Overflow +Info	2014-07-20	2017-12-08	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</p>														
6	CVE-2014-0118	399		DoS	2014-07-20	2017-12-08	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.</p>														
7	CVE-2014-0117	20		DoS	2014-07-20	2016-07-08	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.</p>														
8	CVE-2014-0098	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.</p>														
9	CVE-2013-6438	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.</p>														
10	CVE-2013-4352			DoS	2014-07-20	2014-08-04	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.</p>														

PHP » PHP » 5.4.16 RC1 : Security Vulnerabilities

Cpe Name: cpe:/a:php:php:5.4.16:rc1

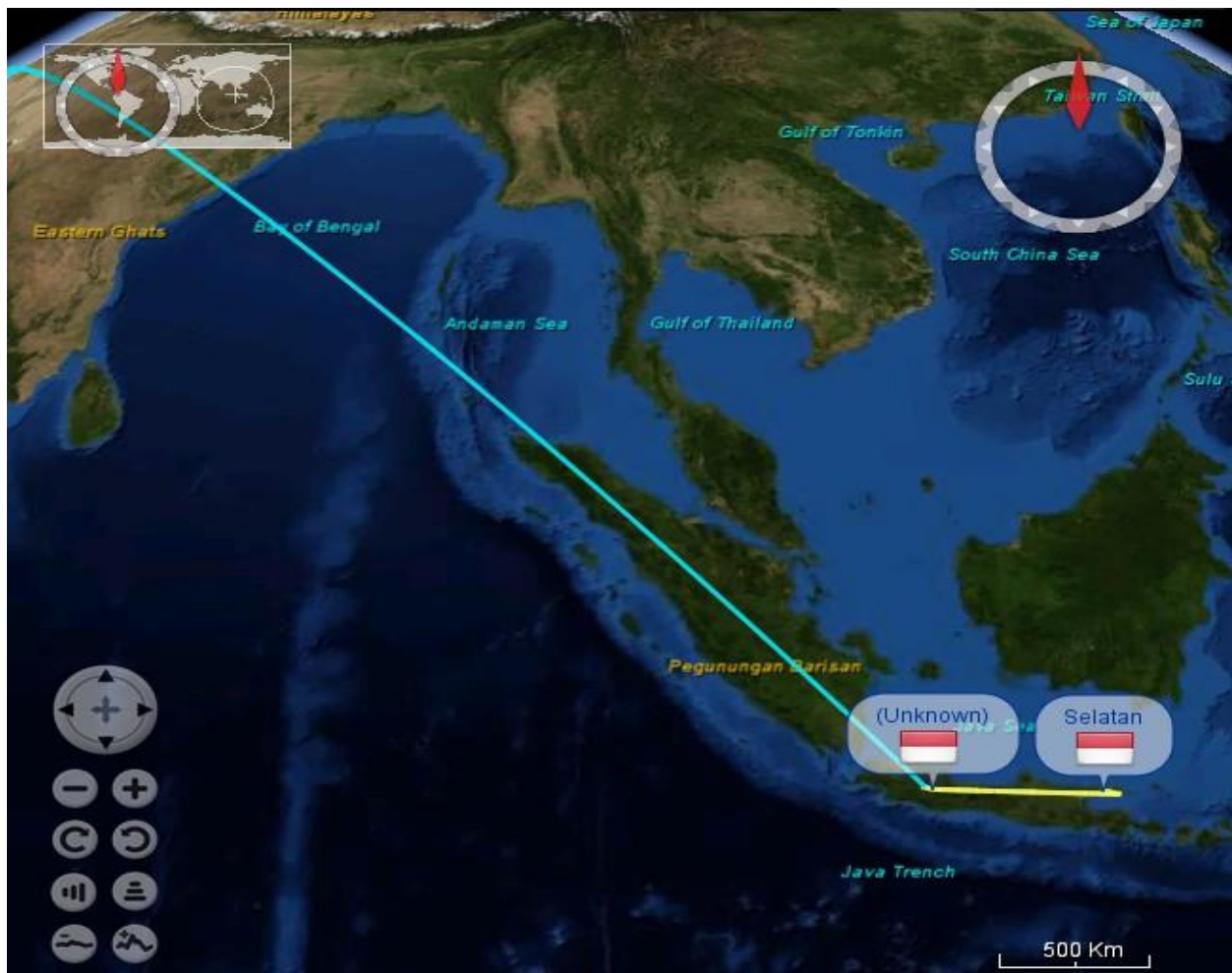
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

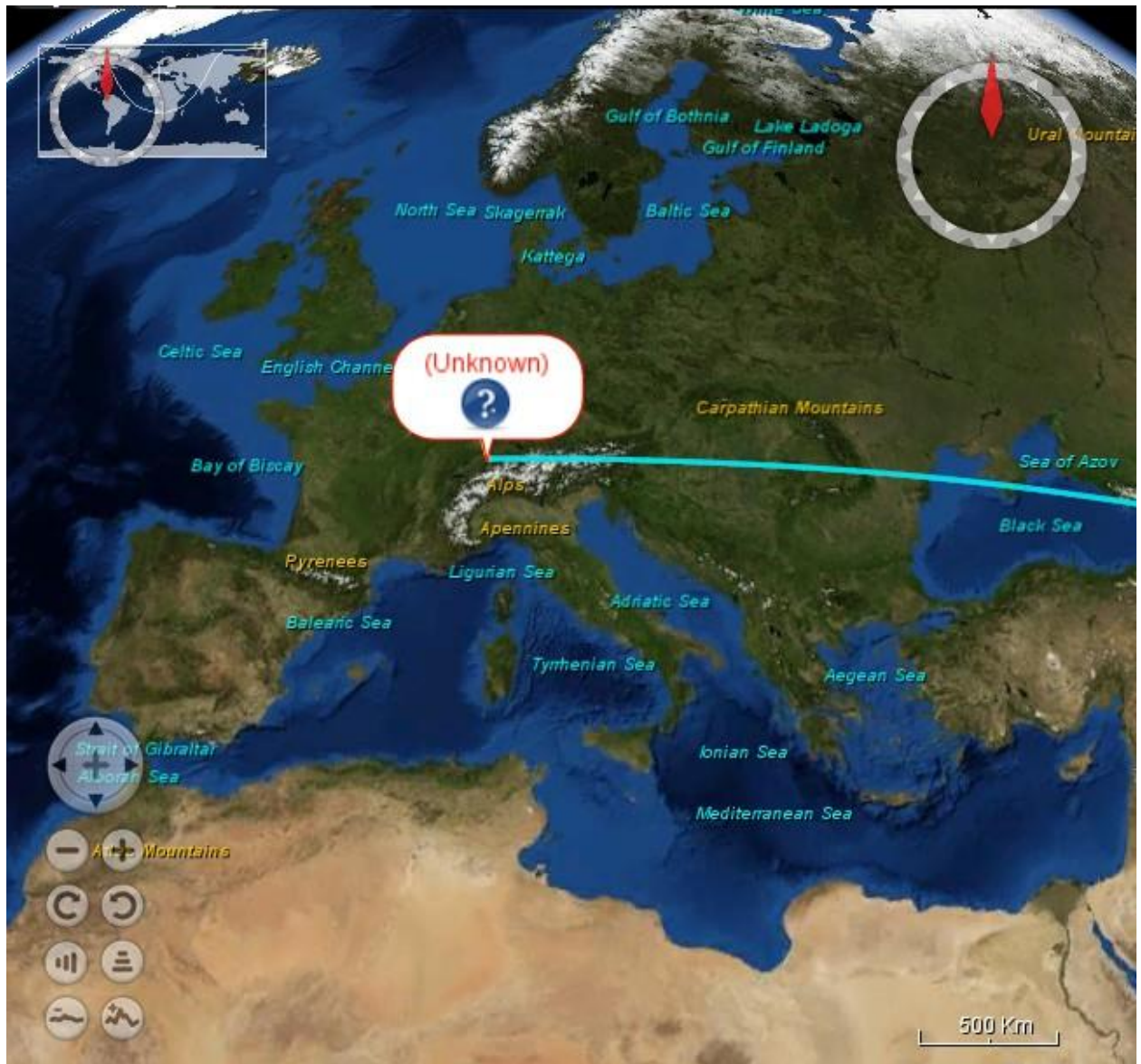
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-19935	476		DoS	2018-12-07	2018-12-31	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.</p>														
2	CVE-2018-19396	20		DoS	2018-11-20	2019-01-02	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.</p>														
3	CVE-2018-19395	476		DoS	2018-11-20	2018-12-27	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safefarray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScrip.Shell").</p>														
4	CVE-2018-17082	79		XSS	2018-09-16	2018-12-11	4.3	None	Remote	Medium	Not required	None	Partial	None
<p>The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.</p>														
5	CVE-2018-15132	200		+Info	2018-08-07	2018-11-08	5.0	None	Remote	Low	Not required	Partial	None	None
<p>An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.</p>														
6	CVE-2018-14883	190		Overflow	2018-08-03	2018-12-11	5.0	None	Remote	Low	Not required	None	None	Partial
<p>An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.</p>														
7	CVE-2018-10549	125			2018-04-29	2018-12-03	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_if_add_value mishandles the case of a MakerNote that lacks a final '\0' character.</p>														
8	CVE-2018-10548	476		DoS	2018-04-29	2018-12-03	5.0	None	Remote	Low	Not required	None	None	Partial
<p>An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_if_add_value mishandles the case of a MakerNote that lacks a final '\0' character.</p>														

Traceroute





2. www.tokopedia.com

Network

- Site : <http://www.tokopedia.co.id>
- Domain : tokopedia.co.id
- IP address : 103.3.61.107
- Ipv6 Address : -
- Domain Registrar : -
- Organisation : -
- Top level domain : Indonesia (.co.id)
- Hosting country :  [US](#)
- Netblock Owner : [Dynamic Network Services, Inc.](#)
- Nameserver : -
- DNS admin : -
- Reverse DNS : -
- Nameserver organisation : -
- Hosting company : -
- DNS Security Extensions :-

Registrar Information

- Domain ID:PANDI-DO47626
- Domain Name:TOKOPEDIA.CO.ID
- Created On:09-Oct-2009 13:23:17 UTC
- Last Updated On:23-Sep-2018 02:57:06 UTC
- Expiration Date:10-Oct-2020 23:59:59 UTC
- Status:ok
- Sponsoring Registrar Organization:CORE MEDIATECH
- Sponsoring Registrar City:Jakarta
- Sponsoring Registrar State/Province:DKI Jakarta
- Sponsoring Registrar Postal Code:13150
- Sponsoring Registrar Country:ID
- Sponsoring Registrar Phone:02128507000
- Sponsoring Registrar Website:<http://iddomain.dnet.net.id>
- Sponsoring Registrar Contact Email:hostmaster@dnet.net.id
- Name Server:NS1.P21.DYNECT.NET
- Name Server:NS2.P21.DYNECT.NET
- Name Server:NS3.P21.DYNECT.NET
- Name Server:NS4.P21.DYNECT.NET
- DNSSEC:Unsigned

Hosting

- [Dynamic Network Services, Inc. 150 Dow St. Manchester NH US 03101](#)
 - IP address : 216.146.46.10
 - OS : FreeBSD
 - Webserver : nginx/1.6.2
 - Tanggal : 21-May-2017

CVE

[Nginx](#) » [Nginx](#) » [1.6.2: Security Vulnerabilities](#)

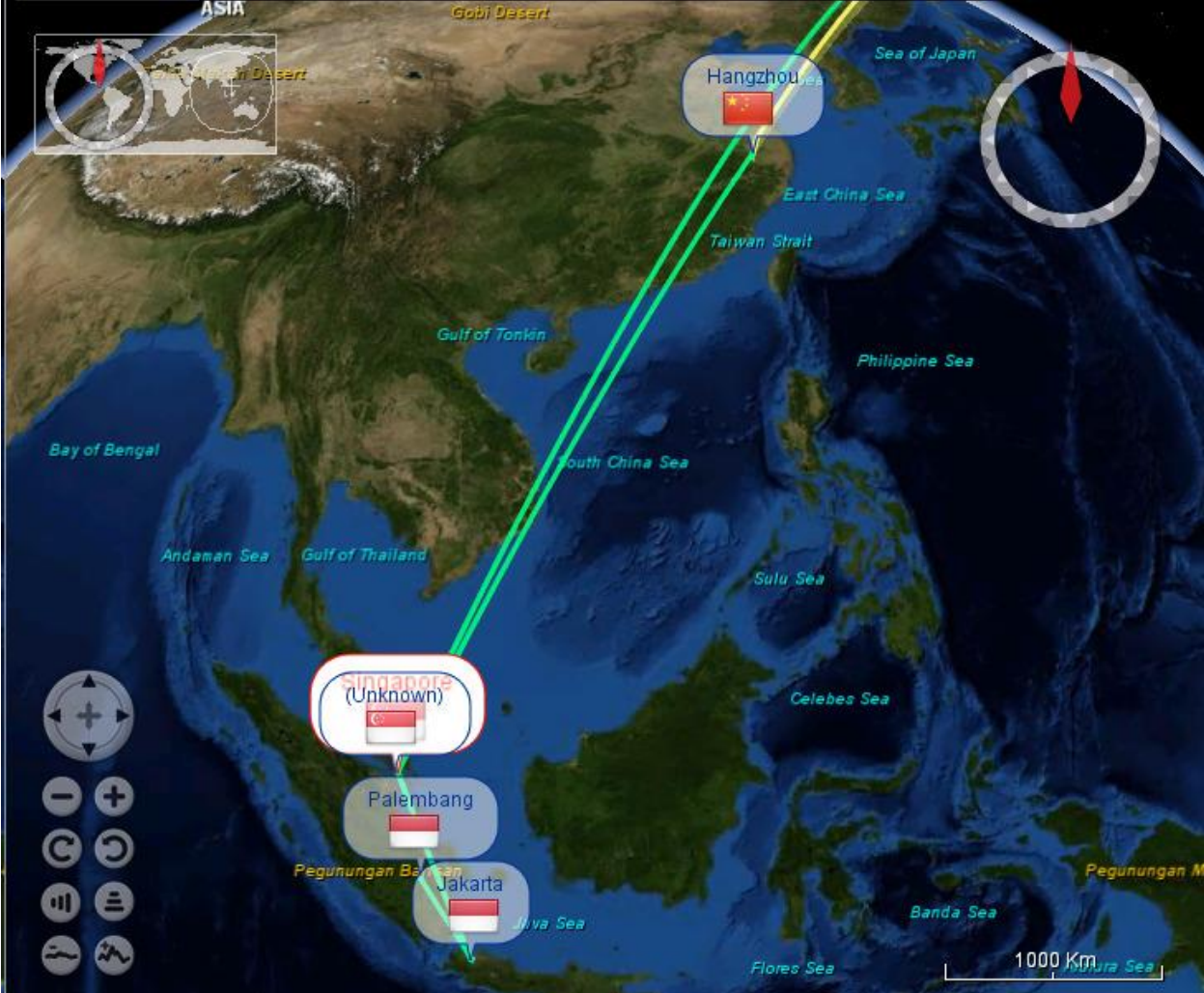
Cpe Name: `cpe:/a/nginx/nginx:1.6.2`
CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)
Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)
[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-16844	400			2018-11-07	2018-12-12	7.8	None	Remote	Low	Not required	None	None	Complete
<small>nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.</small>														
2	CVE-2016-1247	59		+Priv	2016-11-29	2018-10-09	7.2	Admin	Local	Low	Not required	Complete	Complete	Complete
<small>The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx ebuild before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.</small>														
3	CVE-2016-0746			DoS	2016-02-15	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<small>Use-after-free vulnerability in the resolver in nginx 0.6.18 through 1.8.0 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.</small>														

Total number of vulnerabilities : 3 Page : [1](#) (This Page)

Traceroute







3. www.indonesia.go.id

Network

- Site : <http://www.indonesia.go.id>
- Domain : indonesia.go.id
- IP address : 202.89.117.193
- Ipv6 Address : -
- Domain Registrar : -
- Organisation : -
- Top level domain : Indonesia (.go.id)
- Hosting country :  [ID](#)
- Netblock Owner : [Kementerian Komunikasi dan Informasi Republik Indonesia](#)
- Nameserver : ns1.setneg.go.id
- DNS admin : hostmaster@ns1.setneg.go.id
- Reverse DNS : -
- Nameserver organisation : -
- Hosting company : Kementerian Komunikasi dan Informatika
Republik Indonesia
- DNS Security Extensions :-

Registrar Information

- Domain Name: indonesia.go.id
- Top Level Domain: ID (Indonesia)
- Domain ID:PANDI-DO53077
- Domain Name:INDONESIA.GO.ID
- Created On:10-May-2000 13:23:32 UTC
- Last Updated On:08-Jan-2019 07:42:19 UTC
- Expiration Date:01-Feb-2021 23:59:59 UTC
- Status:ok
- Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
- Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
- Sponsoring Registrar City:Jakarta Pusat
- Sponsoring Registrar State/Province:Jakarta
- Sponsoring Registrar Postal Code:10110

- Sponsoring Registrar Country:ID
- Sponsoring Registrar Phone:622138433507
- Sponsoring Registrar Website:domain.go.id
- Sponsoring Registrar Contact Email:hostmaster@pandi.id
- Name Server:NS1.SETNEG.GO.ID
- Name Server:NS2.SETNEG.GO.ID
- DNSSEC:Unsigned

Hosting

- [Kementerian Komunikasi dan Informasi Republik Indonesia Government / Direct Member IDNIC Jl. Medan Merdeka Barat no. 9 Jakarta Pusat, 10110](#)
 - IP address : 202.89.117.193
 - OS : Linux
 - Webserver : Apache/2.4.6 CentOS OpenSSL/1.0.2k-fips PHP/5.6.36
 - Tanggal : 10-Feb-2019

Site Technology

- Application Servers : CentOS,Apache
- Server-Side : PHP,SSL, PHP Enabled
- Client-side : JavaScript
- Client-Side Scripting Frameworks : jQuery, Bootstrap Javascript Library
- PHP Application : PHP Application, CodeIgniter Framework
- Tools : OpenSSL
- Character Encoding : UTF8
- Web Browser Targeting : Document Compatibility Mode
- Doctype : HTML5,HTML
- HTML 5 : Video Tak, Viewport meta tag
- CSS Usage : External,embedded

CVE

Apache » Http Server » 2.4.6 : Security Vulnerabilities (Denial Of Service)

Cpe Name: cpe:/a:apache:http_server:2.4.6

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15710	787		DoS	2018-03-26	2018-11-13	5.0	None	Remote	Low	Not required	None	None	Partial
<p>In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.</p>														
2	CVE-2017-9788	20		DoS +Info	2017-07-13	2018-01-04	6.4	None	Remote	Low	Not required	Partial	None	Partial
<p>In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.</p>														
3	CVE-2014-3523	399		DoS	2014-07-20	2018-01-04	5.0	None	Remote	Low	Not required	None	None	Partial
<p>Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.</p>														
4	CVE-2014-0231	399		DoS	2014-07-20	2018-10-30	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.</p>														
5	CVE-2014-0226	362	1	DoS Exec Code Overflow +Info	2014-07-20	2017-12-08	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/luarequest.c.</p>														
6	CVE-2014-0118	399		DoS	2014-07-20	2017-12-08	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.</p>														
7	CVE-2014-0117	20		DoS	2014-07-20	2016-07-08	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.</p>														
8	CVE-2014-0098	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.</p>														
9	CVE-2013-6438	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
<p>The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.</p>														
10	CVE-2013-4352			DoS	2014-07-20	2014-08-04	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.</p>														

Openssl » Openssl » 1.0.2k : Security Vulnerabilities

Cpe Name: cpe:/a:openssl:openssl:1.0.2k

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-0739	400		DoS	2018-03-27	2019-01-16	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).</p>														
2	CVE-2018-0737	310			2018-04-16	2019-01-16	4.3	None	Remote	Medium	Not required	Partial	None	None
<p>The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).</p>														
3	CVE-2018-0732	320		DoS	2018-06-12	2019-01-19	5.0	None	Remote	Low	Not required	None	None	Partial
<p>During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).</p>														
4	CVE-2017-3738	200		Overflow +Info	2017-12-07	2019-01-16	4.3	None	Remote	Medium	Not required	Partial	None	None
<p>There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</p>														

5	CVE-2017-3737	388		2017-12-07	2018-08-08	4.3	None	Remote	Medium	Not required	Partial	None	None
<p>OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</p>													
6	CVE-2017-3736	200	+Info	2017-11-02	2019-01-16	4.0	None	Remote	Low	Single system	Partial	None	None
<p>There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</p>													
7	CVE-2017-3735	119	Overflow	2017-08-28	2019-01-16	5.0	None	Remote	Low	Not required	None	Partial	None
<p>While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.</p>													

PHP » PHP » 5.6.3 : Security Vulnerabilities

Cpe Name: [cpe:/a:php:php:5.6.3](#)

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

Total number of vulnerabilities : [111](#) Page : [1](#) (This Page) [2](#) [3](#)

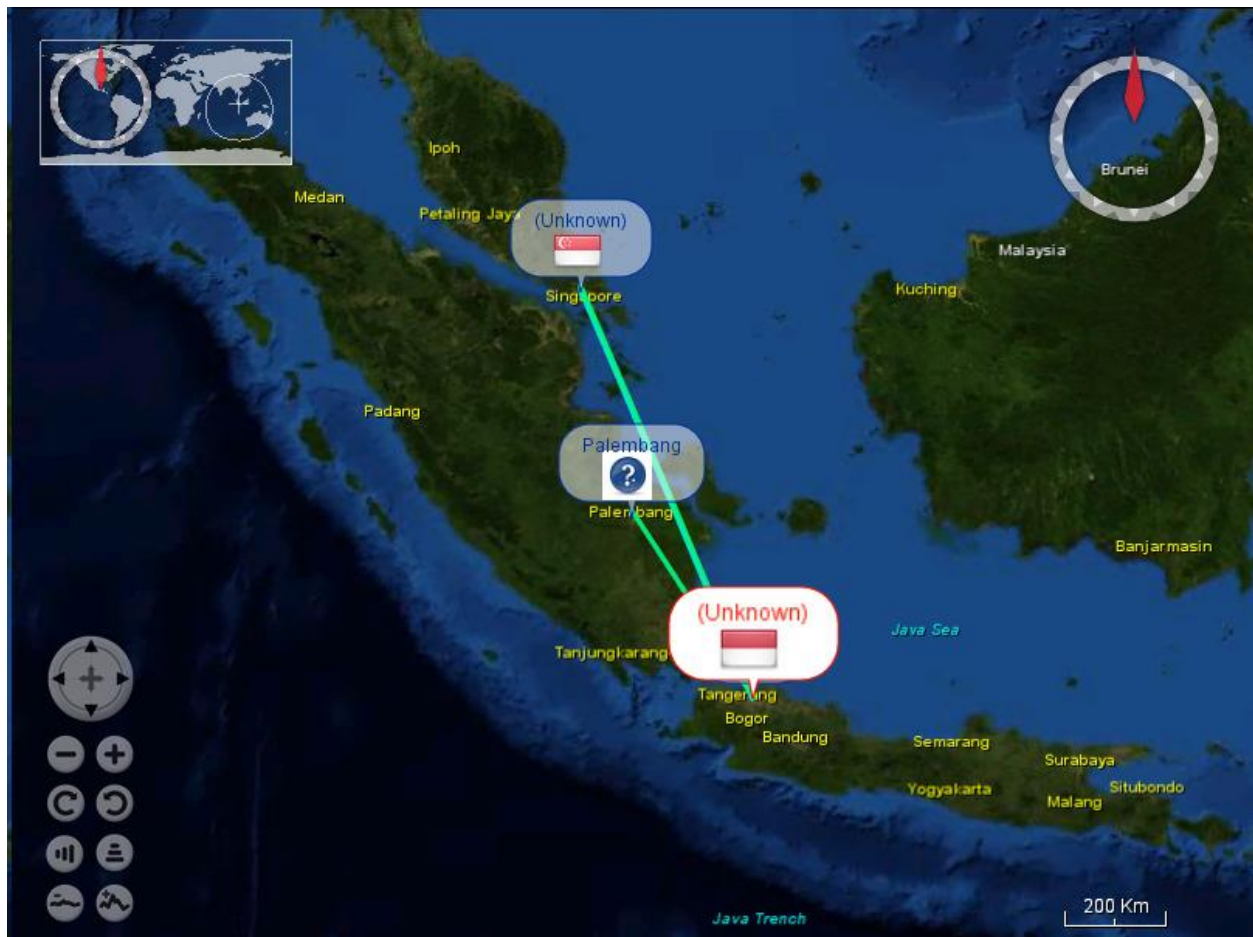
[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-19935	476		DoS	2018-12-07	2018-12-31	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.</p>														
2	CVE-2018-19396	20		DoS	2018-11-20	2019-01-02	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.</p>														
3	CVE-2018-19395	476		DoS	2018-11-20	2018-12-27	5.0	None	Remote	Low	Not required	None	None	Partial
<p>ext/standard/varc in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").</p>														
4	CVE-2018-17082	79		XSS	2018-09-16	2018-12-11	4.3	None	Remote	Medium	Not required	None	Partial	None
<p>The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.</p>														
5	CVE-2018-15132	200		+Info	2018-08-07	2018-11-08	5.0	None	Remote	Low	Not required	Partial	None	None
<p>An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.</p>														
6	CVE-2018-14883	190		Overflow	2018-08-03	2018-12-11	5.0	None	Remote	Low	Not required	None	None	Partial
<p>An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.</p>														
7	CVE-2018-10549	125			2018-04-29	2018-12-03	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_if_add_value mishandles the case of a MakerNote that lacks a final '\0' character.</p>														
8	CVE-2018-10548	476		DoS	2018-04-29	2018-12-03	5.0	None	Remote	Low	Not required	None	None	Partial
<p>An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.</p>														
9	CVE-2018-10547	79		XSS	2018-04-29	2018-09-19	4.3	None	Remote	Medium	Not required	None	Partial	None
<p>An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.</p>														
10	CVE-2018-10546	400			2018-04-29	2018-12-03	5.0	None	Remote	Low	Not required	None	None	Partial
<p>An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.</p>														
11	CVE-2018-10545	200		Bypass +Info	2018-04-29	2018-12-03	1.9	None	Local	Medium	Not required	Partial	None	None
<p>An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcode access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.</p>														
12	CVE-2017-16642	125		+Info	2017-11-07	2018-11-24	5.0	None	Remote	Low	Not required	Partial	None	None
<p>In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.</p>														
13	CVE-2016-10712	20			2018-02-09	2018-03-20	5.0	None	Remote	Low	Not required	None	Partial	None
<p>In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "\$uri = stream_get_meta_data(fopen(\$file, 'r'))['uri']" call mishandles the case where \$file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.</p>														
14	CVE-2016-6297	119		DoS Overflow	2016-07-25	2018-01-04	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.</p>														
15	CVE-2016-6296	119		DoS Overflow	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.</p>														
16	CVE-2016-6295	416		DoS	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.</p>														

16	CVE-2016-6295	416	DoS	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.</p>													
17	CVE-2016-6294	125	DoS	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.</p>													
18	CVE-2016-6292	476	DoS	2016-07-25	2018-01-04	4.3	None	Remote	Medium	Not required	None	None	Partial
<p>The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.</p>													
19	CVE-2016-6291	119	DoS Overflow Mem. Corr. +Info	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>The exif_process_ifd_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.</p>													
20	CVE-2016-6290	416	DoS	2016-07-25	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.</p>													
21	CVE-2016-6289	190	DoS Overflow	2016-07-25	2018-01-04	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.</p>													
22	CVE-2016-5773	416	DoS Exec Code	2016-08-07	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.</p>													
23	CVE-2016-5772	415	DoS Exec Code	2016-08-07	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.</p>													
24	CVE-2016-5771	416	DoS Exec Code	2016-08-07	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.</p>													

[Go to Settings to activate Windows.](#)

Traceroute



#	Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1	Indonesia	Palembang	-2.9167	104.75	192.168.100.1		1	~	0	🕒
2	Indonesia	Palembang	-2.9167	104.75	10.37.0.1		6	~	0	🕒
3	*	*	-2.9167	104.75	*	*	0	<1	0	🕒
4	*	*	-2.9167	104.75	172.16.2.249		15	~	0	🕒
5	*	*	-2.9167	104.75	*	*	0	<1	0	🕒
5	*	*	-2.9167	104.75	*	*	0	<1	0	🕒
7	Indonesia	Jakarta	-6.1744	106.8294	218.100.36.25	telin.openixp.net	27	~	429	🕒
8	Singapore	(Unknown)	1.3667	103.8	180.240.193....		14	~	904	🕒
9	Indonesia	(Unknown)	-6.175	106.8286	202.89.117.1....		30	~	904	🕒