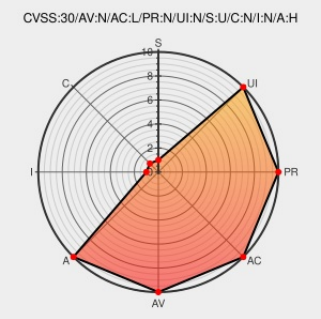
CVE-2017-11144

Published on: 07/10/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

CVE-2017-11144

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Php from Php contain the following vulnerability:

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.

CVE-2017-11144 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4080-1 php7.0	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-4080
208.43.231.11 Git - php-src.git/commit	Mailing List	CONFIRM git.php.net/?p=php-

	Third Party Advisory git.php.net text/xml	src.git;a=commit;h=73cabfedf519298e1a11192699f44d53c529315e
oss-security - Re: CVE IDs needed for PHP vulnerabilites (affects 5.6.30 and 7.0.20)	Mailing List openwall.com text/html	CONFIRM openwall.com/lists/oss-security/2017/07/10/6
PHP: PHP 7 ChangeLog	Release Notes Vendor Advisory php.net text/html	CONFIRM php.net/ChangeLog-7.php
PHP :: Sec Bug #74651 :: negative-size-param (-1) in memcpy in zif_openssl_seal()	Third Party Advisory bugs.php.net application/octet-stream	CONFIRM bugs.php.net/bug.php?id=74651
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1296
Debian -- Security Information -- DSA-4081-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-4081
[R1] SecurityCenter 5.3.2, 5.4.0, 5.4.2, 5.4.5, 5.5.0, and 5.5.1 Fixes Multiple Vulnerabilities - Security Advisory | Tenable™	www.tenable.com text/html	CONFIRM www.tenable.com/security/tns-2017-12
208.43.231.11 Git - php-src.git/commit	Mailing List Third Party Advisory git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=91826a311dd37f4c4e5d605fa7af331e80ddd4c3
208.43.231.11 Git - php-src.git/commit	Mailing List Third Party Advisory git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=89637c6b41b510c20d262c17483f582f115c66d6
PHP: PHP 5 ChangeLog	Release Notes Vendor Advisory php.net text/html	CONFIRM php.net/ChangeLog-5.php
September 2017 PHP Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20180112-0001/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All

Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.17	All	All	All
Application	Php	Php	7.0.18	All	All	All
Application	Php	Php	7.0.19	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.20	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All
Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	7.1.3	All	All	All
Application	Php	Php	7.1.4	All	All	All
Application	Php	Php	7.1.5	All	All	All
Application	Php	Php	7.1.6	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.17	All	All	All
Application	Php	Php	7.0.18	All	All	All

Application	Php	Php	7.0.19	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.20	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All
Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	7.1.3	All	All	All
Application	Php	Php	7.1.4	All	All	All
Application	Php	Php	7.1.5	All	All	All
Application	Php	Php	7.1.6	All	All	All
Application	Php	Php	All	All	All	All

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.6:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.7:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.8:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.9:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.0:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.1:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.4:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.5:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.1.6:*:*:*:*:*:*:*

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→