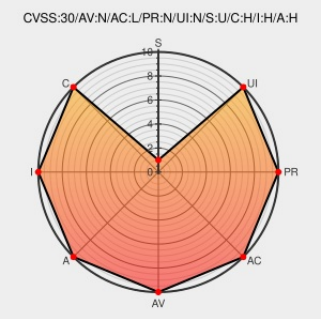
CVE-2015-4116

Published on: 05/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4116

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



Certain versions of Leap from Opensuse contain the following vulnerability:

Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

CVE-2015-4116 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
208.43.231.11 Git - php-src.git/commit	git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=1cbd25ca15383394ffa9ee8601c5de4c0f2f90e1
openSUSE-SU-2016:1524-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1524

File Not Found	Exploit www.htbridge.com text/html Inactive Link Not Archived	MISC www.htbridge.com/advisory/HTB23262
PHP: PHP 5 ChangeLog	php.net text/html	CONFIRM php.net/ChangeLog-5.php
PHP :: Bug #69737 :: Segfault when SplMinHeap::compare produces fatal error	Exploit bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=69737

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Application	Php	Php	5.6.0	All	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	5.6.0	All	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All

Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	All	All	All	All

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.9:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→