

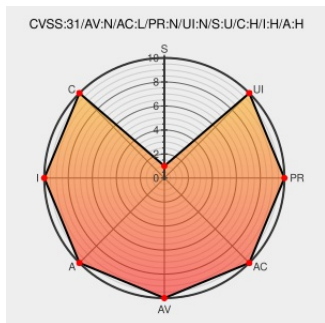


CVE-2016-4346

Published on: 05/21/2016 12:00:00 AM UTC

Last Modified on: 07/20/2022 04:56:00 PM UTC

CVE-2016-4346

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Leap](#) from [Opensuse](#) contain the following vulnerability:

Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.

CVE-2016-4346 has been assigned by [M](#) 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
openSUSE-SU-2016:1357-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1357
PHP :: Sec Bug #71637 :: Multiple Heap Overflow due to integer overflows xml/filter_url/addslashes	Exploit bugs.php.net	CONFIRM bugs.php.net/bug.php?id=71637

[text/html](#)

PHP: PHP 7 ChangeLog

[php.net](#) [CONFIRM php.net/ChangeLog-7.php](#)[text/html](#)

oss-security - [CVE Requests] PHP issues

[www.openwall.com](#)[text/html](#) [MLIST \[oss-security\] 20160428 \[CVE Requests\] PHP issues](#)

openSUSE-SU-2016:1524-1: moderate: Security update for php5

[lists.opensuse.org](#)[text/html](#) [SUSE openSUSE-SU-2016:1524](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Php	Php	All	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:o:opensuse:opensuse:13.2:*****:						
cpe:2.3:a:php:php:*****:						
cpe:2.3:a:php:php:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

