



CVE-2016-4344

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

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

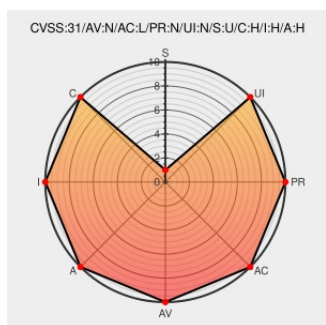
CVE-2016-4344

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Integer overflow in the `xml_utf8_encode` function in `ext/xml/xml.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 argument to the `utf8_encode` function, leading to a heap-based buffer overflow.

CVE-2016-4344 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
PHP :: Sec Bug #71637 :: Multiple Heap Overflow due to integer overflows <code>xml/filter_url/addslashes</code>	Exploit bugs.php.net text/html	php CONFIRM bugs.php.net/bug.php?id=71637
PHP: PHP 7 ChangeLog	php.net	php CONFIRM php.net/ChangeLog-7.php

