

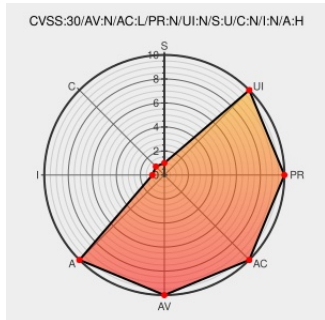


CVE-2016-7416

Published on: 09/17/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

CVE-2016-7416

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

Certain versions of [Php](#) from [Php](#) contain the following vulnerability: ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.

CVE-2016-7416 has been assigned by [M](#) 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
PHP Multiple Memory Corruption Errors Let Remote and Local Users Execute Arbitrary Code on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTrack 1036836

PHP :: Sec Bug #73007 :: SEH buffer overflow msgfmt_format_message	Exploit Issue Tracking bugs.php.net text/html	 CONFIRM bugs.php.net/bug.php?id=73007
[R6] SecurityCenter 5.4.1 Fixes Multiple Vulnerabilities - Security Advisory Tenable Network Security	www.tenable.com text/html	 CONFIRM www.tenable.com/security/tns-2016-19
PHP CVE-2016-7416 Stack Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 93008
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2018:1296
Fix bug #73007: add locale length check · php/php-src@6d55ba2 · GitHub	Issue Tracking Patch github.com text/html	 CONFIRM github.com/php/php-src/commit/6d55ba265637d6adf0ba7e9c9ef11187d1ec2f5b?w=1
oss-security - Re: CVE assignment for PHP 5.6.26 and 7.0.11	Mailing List www.openwall.com text/html	 MLIST [oss-security] 20160915 Re: CVE assignment for PHP 5.6.26 and 7.0.11
PHP: PHP 7 ChangeLog	Release Notes www.php.net text/html	 CONFIRM www.php.net/ChangeLog-7.php
PHP: PHP 5 ChangeLog	Release Notes www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201611-22

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
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	7.0.2	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	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.2	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	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:7.0.2:*:*:*:*:*:						
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:7.0.0:*:*:*:*:*:						
cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:						
cpe:2.3:a:php:php:7.0.10:*:*:*:*:*:						
cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:						
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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)