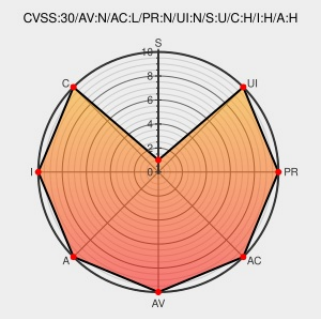
CVE-2016-7134

Published on: 09/11/2016 12:00:00 AM UTC

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

CVE-2016-7134

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



Certain versions of Php from Php contain the following vulnerability:

ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is mishandled in a curl_escape call.

CVE-2016-7134 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
oss-security - Re: CVE assignment for PHP 5.6.25 and 7.0.10 - and libcurl	Mailing List, openwall.com, text/html	MLIST [oss-security] 20160902 Re: CVE assignment for PHP 5.6.25 and 7.0.10 - and libcurl
PHP :: Sec Bug #72674 :: Heap overflow in	Release Notes	CONFIRM bugs.php.net/bug.php?id=72674

curl_escape	bugs.php.net text/html	
PHP CVE-2016-7134 Heap Based Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 92766
Fix bug #72674 - check both curl_escape and curl_unescape · php/php-src@72dbb7f · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/php/php-src/commit/72dbb7f416160f490c4e9987040989a10ad431c7?w=1
PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036680
PHP: PHP 7 ChangeLog	Release Notes www.php.net text/html	CONFIRM www.php.net/ChangeLog-7.php
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201611-22

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	7.0.2	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	7.0.2	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

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

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

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

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:7.0.2:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report