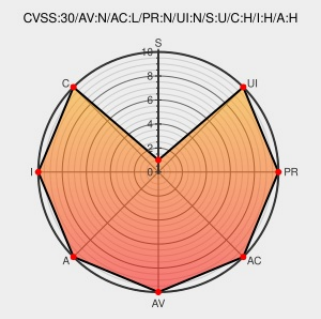
CVE-2016-6294

Published on: 07/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:12 PM UTC

CVE-2016-6294

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



Certain versions of Php from Php contain the following vulnerability:

The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.

CVE-2016-6294 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
About the security content of macOS Sierra 10.12 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT207170
PHP: PHP 7 ChangeLog	Release Notes	CONFIRM php.net/ChangeLog-7.php

PHP : PHP 7 ChangeLog	Release Notes php.net text/html	CONFIRM php.net/ChangeLog-7.php
APPLE-SA-2016-09-20 macOS Sierra 10.12	lists.apple.com text/html	APPLE APPLE-SA-2016-09-20
Debian -- Security Information -- DSA-3631-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-3631
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036430
72.52.91.13 Git - php-src.git/commit	Issue Tracking Patch git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=aa82e99ed8003c01f1ef4f0940e56b85c5b032d4
PHP :: Sec Bug #72533 :: locale_accept_from_http out-of-bounds access	Exploit Issue Tracking Mitigation Patch Third Party Advisory bugs.php.net text/html	CONFIRM bugs.php.net/72533
PHP: PHP 5 ChangeLog	Release Notes php.net text/html	CONFIRM php.net/ChangeLog-5.php
oss-security - Re: Fwd: CVE for PHP 5.5.38 issues	Mailing List openwall.com text/html	MLIST [oss-security] 20160724 Re: Fwd: CVE for PHP 5.5.38 issues
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201611-22
PHP CVE-2016-6294 Local Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 92115

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	5.6.0	alpha1	All	All
Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All

Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.23	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	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	7.0.8	All	All	All
Application	Php	Php	5.6.0	alpha1	All	All
Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.23	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	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	7.0.8	All	All	All
Application	Php	Php	All	All	All	All

- cpe:2.3:a:php:php:5.6.0:alpha1:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:alpha2:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:alpha3:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:alpha4:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:alpha5:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:beta1:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:beta2:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:beta3:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.0:beta4:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.1:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.10:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.11:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.12:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.13:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.14:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.15:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.16:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.17:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.18:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.19:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.2:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.20:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.21:*:*:*:*:*:*:*:
- cpe:2.3:a:php:php:5.6.22:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.23:*:*:*:*:*:*:*:

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: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:7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:alpha3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:alpha4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:alpha5:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:beta4:*:*:*:*:*:*:

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

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

cpe:2.3:a:php:php:5.6.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.19:*:*:*:*:*:*:*:

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

cpe:2.3:a:php:php:5.6.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.21:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.22:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.23:*:*:*:*:*:*:*:

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: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:7.0.8:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→