



CVE-2016-6296

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-6296
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-25 14:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP be

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)						
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	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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
[SECURITY] [DLA 2011-1] xmlrpc-epi security update				af88:00000000000000000000000000000000
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security				af88:00000000000000000000000000000000
PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker				af88:00000000000000000000000000000000
About the security content of macOS Sierra 10.12 - Apple Support				af88:00000000000000000000000000000000
PHP '/xmlrpc/libxmlrpc/simplestring.c' Heap Buffer Overflow Vulnerability				af88:00000000000000000000000000000000
PHP: PHP 7 ChangeLog				af88:00000000000000000000000000000000

Debian -- Security Information -- DSA-3631-1 php5	af8:
oss-security - Re: Fwd: CVE for PHP 5.5.38 issues	af8:
APPLE-SA-2016-09-20 macOS Sierra 10.12	af8:
208.43.231.11 Git - php-src.git/commit	af8:
PHP :: Sec Bug #72606 :: heap-buffer-overflow (write) simplestring_addn simplestring.c	af8:
Red Hat Customer Portal	af8:
PHP: PHP 5 ChangeLog	af8:
USN-3059-1: xmlrpc-epi vulnerability Ubuntu	af8:
208.43.231.11 Git - php-src.git/commit	MIT
CVE Program record	CVI
NVD vulnerability detail	NVI

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.