CVE-2016-4073

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

Summary

CVE	CVE-2016-4073
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-20 11:00:18 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x befor

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
Operating System	Apple	Mac Os X	All	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All

Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.18	All	All	All
Application	Php	Php	5.5.19	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.20	All	All	All
Application	Php	Php	5.5.21	All	All	All
Application	Php	Php	5.5.22	All	All	All
Application	Php	Php	5.5.23	All	All	All
Application	Php	Php	5.5.24	All	All	All
Application	Php	Php	5.5.25	All	All	All
Application	Php	Php	5.5.26	All	All	All
Application	Php	Php	5.5.27	All	All	All
Application	Php	Php	5.5.29	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.30	All	All	All
Application	Php	Php	5.5.32	All	All	All
Application	Php	Php	5.5.33	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	5.6.0	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	5.6.3	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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Document Display | HPE Support Center	af854a3a-2127-422b-91ae-364da26
oss-security - Re: CVE request: PHP issues fixed in 7.0.5, 5.6.20 and 5.5.34 releases	af854a3a-2127-422b-91ae-364da26
About the security content of OS X El Capitan v10.11.5 and Security Update 2016-003 - Apple Support	af854a3a-2127-422b-91ae-364da26
71906.diff · GitHub	af854a3a-2127-422b-91ae-364da26
USN-2952-2: PHP regression | Ubuntu	af854a3a-2127-422b-91ae-364da26
Debian -- Security Information -- DSA-3560-1 php5	af854a3a-2127-422b-91ae-364da26

Debian -- Security Information -- DSA-3560-1 php5	af854a3a-2127-422b-91ae-364da26
PHP: PHP 5 ChangeLog	af854a3a-2127-422b-91ae-364da26
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	af854a3a-2127-422b-91ae-364da26
PHP: PHP 7 ChangeLog	af854a3a-2127-422b-91ae-364da26
USN-2952-1: PHP vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da26
APPLE-SA-2016-05-16-4 OS X El Capitan 10.11.5 and Security Update 2016-003	af854a3a-2127-422b-91ae-364da26
[security-announce] openSUSE-SU-2016:1373-1: important: Security update	af854a3a-2127-422b-91ae-364da26
208.43.231.11 Git - php-src.git/commit	af854a3a-2127-422b-91ae-364da26
[security-announce] openSUSE-SU-2016:1274-1: important: Security update	af854a3a-2127-422b-91ae-364da26
PHP :: Sec Bug #71906 :: AddressSanitizer: negative-size-param (-1) in mbfl_strcut	af854a3a-2127-422b-91ae-364da26
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26
[security-announce] SUSE-SU-2016:1277-1: important: Security update for	af854a3a-2127-422b-91ae-364da26
PHP 'libmbfl/mbfl/mbfilter.c' Function Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da26
208.43.231.11 Git - php-src.git/commit	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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