CVE-2016-4537

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

Summary

CVE	CVE-2016-4537
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-22 01:59:21 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a n

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-20 | 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	Fedoraproject	Fedora	24	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Application	Php	Php	5.6.0	All	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	5.6.3	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	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	Li
208.43.231.11 Git - php-src.git/commit	af854a3a-2127-422b-91ae-364da2661108	git
PHP 'bcmath.c' Multiple Local Heap Overflow Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	ww
Document Display | HPE Support Center	af854a3a-2127-422b-91ae-364da2661108	h2
PHP :: Sec Bug #72093 :: bcpowmod accepts negative scale and corrupts _one_ definition	af854a3a-2127-422b-91ae-364da2661108	bu
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	se
oss-security - CVE Request: PHP: several issues fixed with 7.0.6, 5.6.21 and 5.5.35	af854a3a-2127-422b-91ae-364da2661108	ww
Document Display | HPE Support Center	af854a3a-2127-422b-91ae-364da2661108	h2
openSUSE-SU-2016:1357-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364da2661108	list
PHP: PHP 7 ChangeLog	af854a3a-2127-422b-91ae-364da2661108	ph
[SECURITY] Fedora 24 Update: php-5.6.21-1.fc24	af854a3a-2127-422b-91ae-364da2661108	list
Document Display | HPE Support Center	af854a3a-2127-422b-91ae-364da2661108	h2
Debian -- Security Information -- DSA-3602-1 php5	af854a3a-2127-422b-91ae-364da2661108	ww
openSUSE-SU-2016:1524-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364da2661108	list
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhr
PHP: PHP 5 ChangeLog	af854a3a-2127-422b-91ae-364da2661108	ph
208.43.231.11 Git - php-src.git/commit	MITRE	git

CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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