CVE-2007-2511

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

Summary

CVE	CVE-2007-2511
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-09 00:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Buffer overflow in the user_filter_factory_create function in PHP before 5.2.2 has unknown impact and local attack vectors.

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	4.0.0	All	All	All

Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All

Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
osvdb.org/34676	af854a3a-2127-422b-91ae-364da2661108	osvdb.org
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	security.gent
Ubuntu update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
[security-announce] SUSE Security Announcement: php4,php5 (SUSE-SA:2007:	af854a3a-2127-422b-91ae-364da2661108	lists.opensus
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da2661108	www.mandriv
PHP: PHP 5.2.2 Release Announcement	af854a3a-2127-422b-91ae-364da2661108	us2.php.net
Gentoo update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
viewcvs.php.net/viewvc.cgi/php-src/ext/standard/user_filters.c	af854a3a-2127-422b-91ae-364da2661108	viewcvs.php.
www.trustix.org/errata/2007/0017	af854a3a-2127-422b-91ae-364da2661108	www.trustix.c
SUSE update for php4 and php5 - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
USN-462-1: PHP vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubuntu.
Mandriva update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Trustix Updates for Multiple Packages - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-04-02	Mark J Cox	The PHP interpreter does not offer a reliable "sandboxed" security layer (as found in,

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

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

Free CVE JSON API cve.report/api

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