CVE-2014-3515

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

Summary

CVE	CVE-2014-3515
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-09 11:07:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will ha

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

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	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM Security Bulletin: Multiple vulnerabilities in PHP 5.2 open source component for IBM Lotus Protector for Mail Security (CVE-2014-3515 CV
Red Hat Customer Portal
openSUSE-SU-2014:1236-1: moderate: several security fixes for php5
PHP :: Sec Bug #67492 :: unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion
PHP: PHP 5 ChangeLog
About the security content of OS X Mavericks v10.9.5 and Security Update 2014-004 - Apple Support
Oracle Bulletin Board Update - January 2015
Security Advisory SA60998 - IBM Lotus Protector for Mail Security PHP Multiple Vulnerabilities - Secunia
208.43.231.11 Git - php-src.git/commit
Debian -- Security Information -- DSA-2974-1 php5
Red Hat Customer Portal
About Secunia Research | Flexera
PHP unserialize() Function Type Confusion Security Vulnerability
About Secunia Research | Flexera
'[security bulletin] HPSBUX03102 SSRT101681 rev.1 - HP-UX Apache Server Suite running Apache Tomcat o' - MARC
208.43.231.11 Git - php-src.git/commit
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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