CVE-2016-5770

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

Summary

CVE	CVE-2016-5770
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-07 10:59:18 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x b

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-190 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/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 v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/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	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	Link
Document Display | HPE Support Center	af854a3a-2127-422b-91ae-364da2661108	h20566.w
oss-security - Re: CVE for PHP 5.5.37 issues	af854a3a-2127-422b-91ae-364da2661108	www.ope
[security-announce] openSUSE-SU-2016:1761-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108	lists.open
Debian -- Security Information -- DSA-3618-1 php5	af854a3a-2127-422b-91ae-364da2661108	www.deb
PHP :: Sec Bug #72262 :: int/size_t confusion in SplFileObject::fread	af854a3a-2127-422b-91ae-364da2661108	bugs.php
About the security content of macOS Sierra 10.12 - Apple Support	af854a3a-2127-422b-91ae-364da2661108	support.a
Fix bug #72262 - do not overflow int · php/php-src@7245bff · GitHub	af854a3a-2127-422b-91ae-364da2661108	github.co
openSUSE-SU-2016:1922-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364da2661108	lists.open
APPLE-SA-2016-09-20 macOS Sierra 10.12	af854a3a-2127-422b-91ae-364da2661108	lists.apple
PHP 'ext/spl/spl_directory.c' Type Confusion Remote Denial Of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secu

Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redha
PHP: PHP 5 ChangeLog	af854a3a-2127-422b-91ae-364da2661108	php.net
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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