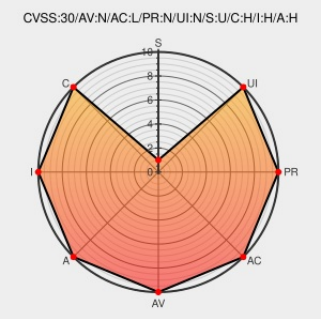
CVE-2016-4542

Published on: 05/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:59 PM UTC

CVE-2016-4542

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

CVE-2016-4542 has been assigned by security@debian.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3602-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-3602

208.43.231.11 Git - php-src.git/commit	git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=082aecfc3a753ad03be82cf14f03ac065723ec92
openSUSE-SU-2016:1357-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1357
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
PHP: PHP 7 ChangeLog	Patch php.net text/html	CONFIRM php.net/ChangeLog-7.php
openSUSE-SU-2016:1524-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1524
PHP :: Sec Bug #72094 :: Out of bounds heap read access in exif header processing	Exploit bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=72094
oss-security - CVE Request: PHP: several issues fixed with 7.0.6, 5.6.21 and 5.5.35	www.openwall.com text/html	MLIST [oss-security] 20160505 CVE Request: PHP: several issues fixed with 7.0.6, 5.6.21 and 5.5.35
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
[SECURITY] Fedora 24 Update: php-5.6.21-1.fc24	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-f4e73663f4
PHP 'ext/exif/exif.c' Multiple Heap Based Buffer Overflow Vulnerabilities	cve.report (archive) text/html	BID 89844
PHP: PHP 5 ChangeLog	Patch php.net text/html	CONFIRM php.net/ChangeLog-5.php
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201611-22

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	24	All	All	All

Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Opensuse	Leap	42.1	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	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

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.6.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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