



CVE-2014-3587

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-3587
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-23 01:55:00 UTC
Updated	2018-01-05 02:29:00 UTC
Description	Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PH

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Christos Zoulas	File	5.00	All	All	All
Application	Christos Zoulas	File	5.01	All	All	All
Application	Christos Zoulas	File	5.02	All	All	All
Application	Christos Zoulas	File	5.03	All	All	All
Application	Christos Zoulas	File	5.04	All	All	All
Application	Christos Zoulas	File	5.05	All	All	All
Application	Christos Zoulas	File	5.06	All	All	All
Application	Christos Zoulas	File	5.07	All	All	All
Application	Christos Zoulas	File	5.08	All	All	All
Application	Christos Zoulas	File	5.09	All	All	All
Application	Christos Zoulas	File	5.10	All	All	All
Application	Christos Zoulas	File	5.11	All	All	All
Application	Christos Zoulas	File	5.12	All	All	All
Application	Christos Zoulas	File	5.13	All	All	All
Application	Christos Zoulas	File	5.14	All	All	All
Application	Christos Zoulas	File	5.15	All	All	All
Application	Christos Zoulas	File	5.16	All	All	All

Application	Christos Zoulas	File	5.17	All	All	All
Application	Christos Zoulas	File	5.18	All	All	All
Application	Christos Zoulas	File	5.00	All	All	All
Application	Christos Zoulas	File	5.01	All	All	All
Application	Christos Zoulas	File	5.02	All	All	All
Application	Christos Zoulas	File	5.03	All	All	All
Application	Christos Zoulas	File	5.04	All	All	All
Application	Christos Zoulas	File	5.05	All	All	All
Application	Christos Zoulas	File	5.06	All	All	All
Application	Christos Zoulas	File	5.07	All	All	All
Application	Christos Zoulas	File	5.08	All	All	All
Application	Christos Zoulas	File	5.09	All	All	All
Application	Christos Zoulas	File	5.10	All	All	All
Application	Christos Zoulas	File	5.11	All	All	All
Application	Christos Zoulas	File	5.12	All	All	All
Application	Christos Zoulas	File	5.13	All	All	All
Application	Christos Zoulas	File	5.14	All	All	All
Application	Christos Zoulas	File	5.15	All	All	All
Application	Christos Zoulas	File	5.16	All	All	All
Application	Christos Zoulas	File	5.17	All	All	All
Application	Christos Zoulas	File	5.18	All	All	All
Application	Christos Zoulas	File	All	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.0	beta2	All	All
Application	Php	Php	5.4.0	beta2	32-bit	All
Application	Php	Php	5.4.0	rc2	All	All
Application	Php	Php	5.4.1	All	All	All
Application	Php	Php	5.4.10	All	All	All
Application	Php	Php	5.4.11	All	All	All
Application	Php	Php	5.4.12	All	All	All
Application	Php	Php	5.4.12	rc1	All	All
Application	Php	Php	5.4.12	rc2	All	All
Application	Php	Php	5.4.13	All	All	All
Application	Php	Php	5.4.13	rc1	All	All
Application	Php	Php	5.4.14	All	All	All

Application	Php	Php	5.4.14	rc1	All	All
Application	Php	Php	5.4.15	All	All	All
Application	Php	Php	5.4.15	rc1	All	All
Application	Php	Php	5.4.16	rc1	All	All
Application	Php	Php	5.4.17	All	All	All
Application	Php	Php	5.4.18	All	All	All
Application	Php	Php	5.4.19	All	All	All
Application	Php	Php	5.4.2	All	All	All
Application	Php	Php	5.4.20	All	All	All
Application	Php	Php	5.4.21	All	All	All
Application	Php	Php	5.4.22	All	All	All
Application	Php	Php	5.4.23	All	All	All
Application	Php	Php	5.4.24	All	All	All
Application	Php	Php	5.4.25	All	All	All
Application	Php	Php	5.4.26	All	All	All
Application	Php	Php	5.4.27	All	All	All
Application	Php	Php	5.4.28	All	All	All
Application	Php	Php	5.4.29	All	All	All
Application	Php	Php	5.4.3	All	All	All
Application	Php	Php	5.4.30	All	All	All
Application	Php	Php	5.4.4	All	All	All
Application	Php	Php	5.4.5	All	All	All
Application	Php	Php	5.4.6	All	All	All
Application	Php	Php	5.4.7	All	All	All
Application	Php	Php	5.4.8	All	All	All
Application	Php	Php	5.4.9	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All

Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.15	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.0	beta2	All	All
Application	Php	Php	5.4.0	beta2	32-bit	All
Application	Php	Php	5.4.0	rc2	All	All
Application	Php	Php	5.4.1	All	All	All
Application	Php	Php	5.4.10	All	All	All
Application	Php	Php	5.4.11	All	All	All
Application	Php	Php	5.4.12	All	All	All
Application	Php	Php	5.4.12	rc1	All	All
Application	Php	Php	5.4.12	rc2	All	All
Application	Php	Php	5.4.13	All	All	All
Application	Php	Php	5.4.13	rc1	All	All
Application	Php	Php	5.4.14	All	All	All
Application	Php	Php	5.4.14	rc1	All	All
Application	Php	Php	5.4.15	All	All	All
Application	Php	Php	5.4.15	rc1	All	All
Application	Php	Php	5.4.16	rc1	All	All

Application	Php	Php	5.4.17	All	All	All
Application	Php	Php	5.4.18	All	All	All
Application	Php	Php	5.4.19	All	All	All
Application	Php	Php	5.4.2	All	All	All
Application	Php	Php	5.4.20	All	All	All
Application	Php	Php	5.4.21	All	All	All
Application	Php	Php	5.4.22	All	All	All
Application	Php	Php	5.4.23	All	All	All
Application	Php	Php	5.4.24	All	All	All
Application	Php	Php	5.4.25	All	All	All
Application	Php	Php	5.4.26	All	All	All
Application	Php	Php	5.4.27	All	All	All
Application	Php	Php	5.4.28	All	All	All
Application	Php	Php	5.4.29	All	All	All
Application	Php	Php	5.4.3	All	All	All
Application	Php	Php	5.4.30	All	All	All
Application	Php	Php	5.4.4	All	All	All
Application	Php	Php	5.4.5	All	All	All
Application	Php	Php	5.4.6	All	All	All
Application	Php	Php	5.4.7	All	All	All
Application	Php	Php	5.4.8	All	All	All
Application	Php	Php	5.4.9	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All

Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.15	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	All	All	All	All

References

Reference	Source	Link
USN-2344-1: PHP vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Oracle Bulletin Board Update - January 2015	CONFIRM	www.oracle.com
Debian -- Security Information -- DSA-3021-1 file	DEBIAN	www.debian.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Fix bug #67716 - Segfault in cdf.c · php/php-src@7ba1409 · GitHub	CONFIRM	github.com
About Secunia Research Flexera	SECUNIA	secunia.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
APPLE-SA-2015-04-08-2 OS X 10.10.3 and Security Update 2015-004	APPLE	lists.apple.com
Oracle Linux Bulletin - April 2016	CONFIRM	www.oracle.com
Prevent wrap around (Remi Collet at redhat) · file/file@0641e56 · GitHub	CONFIRM	github.com
CVE-2014-3587	CONFIRM	security-tracker.debian
PHP :: Sec Bug #67716 :: Segfault in cdf.c	CONFIRM	bugs.php.net
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com
USN-2369-1: file vulnerability Ubuntu	UBUNTU	www.ubuntu.com
PHP 'cdf_read_property_info()' Function CVE-2014-3587 Incomplete Fix Denial of Service Vulnerability	BID	www.securityfocus.com

Security Advisory SA60696 - Debian update for php5 - Secunia	SECUNIA	secunia.com
PHP: PHP 5 ChangeLog	CONFIRM	php.net
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Debian -- Security Information -- DSA-3008-1 php5	DEBIAN	www.debian.org
Oracle Critical Patch Update - October 2017	CONFIRM	www.oracle.com
About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004 - Apple Support	CONFIRM	support.apple.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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