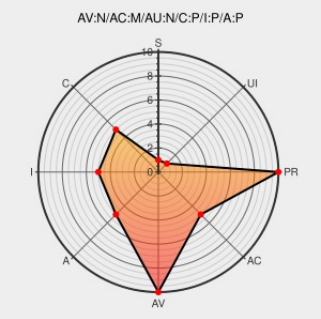
CVE-2013-4113

Published on: 07/13/2013 12:00:00 AM UTC

Last Modified on: 08/16/2022 01:29:00 PM UTC

CVE-2013-4113

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



Certain versions of Php from Php contain the following vulnerability:

ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.

CVE-2013-4113 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Security Advisory SA54163 - Debian update for php5 - Secunia	web.archive.org text/html	SECUNIA 54163
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1061
About the security content of OS X Mavericks v10.9.2 and Security Update 2014-001 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT6150
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 54104
[security-announce] SUSE-SU-2013:1285-1: important: Security update	lists.opensuse.org text/html	SUSE SUSE-SU-2013:1285

for		
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1063
Bug 983689 – CVE-2013-4113 php: xml_parse_into_struct buffer overflow when parsing deeply nested XML	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=983689
[security-announce] SUSE-SU-2013:1315-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2013:1315
PHP :: Sec Bug #65236 :: heap corruption in xml parser	bugs.php.net text/xml	CONFIRM bugs.php.net/bug.php?id=65236
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1049
Security Advisory SA54165 - Red Hat update for php - Secunia	web.archive.org text/html	SECUNIA 54165
USN-1905-1: PHP vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1905-1
Debian -- Security Information -- DSA-2723-1 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-2723
208.43.231.11 Git - php-src.git/commit	Patch git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=7d163e8a0880ae8af2dd869071393e5dc07ef271
[security-announce] SUSE-SU-2013:1316-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2013:1316
PHP: News Archive - 2013	php.net text/html	CONFIRM php.net/archive/2013.php#id2013-07-11-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1062
PHP: PHP 5 ChangeLog	php.net text/html	CONFIRM php.net/ChangeLog-5.php
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1050
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 54071

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	All	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.10	All	All	All
Application	Php	Php	5.3.11	All	All	All
Application	Php	Php	5.3.12	All	All	All
Application	Php	Php	5.3.13	All	All	All
Application	Php	Php	5.3.14	All	All	All
Application	Php	Php	5.3.15	All	All	All
Application	Php	Php	5.3.16	All	All	All
Application	Php	Php	5.3.17	All	All	All
Application	Php	Php	5.3.18	All	All	All
Application	Php	Php	5.3.19	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.20	All	All	All
Application	Php	Php	5.3.21	All	All	All
Application	Php	Php	5.3.22	All	All	All
Application	Php	Php	5.3.23	All	All	All
Application	Php	Php	5.3.24	All	All	All
Application	Php	Php	5.3.25	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.10	All	All	All
Application	Php	Php	5.3.11	All	All	All
Application	Php	Php	5.3.12	All	All	All
Application	Php	Php	5.3.13	All	All	All
Application	Php	Php	5.3.14	All	All	All

Application	Php	Php	5.3.14	All	All	All
Application	Php	Php	5.3.15	All	All	All
Application	Php	Php	5.3.16	All	All	All
Application	Php	Php	5.3.17	All	All	All
Application	Php	Php	5.3.18	All	All	All
Application	Php	Php	5.3.19	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.20	All	All	All
Application	Php	Php	5.3.21	All	All	All
Application	Php	Php	5.3.22	All	All	All
Application	Php	Php	5.3.23	All	All	All
Application	Php	Php	5.3.24	All	All	All
Application	Php	Php	5.3.25	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	All	All	All	All

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

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.21:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.22:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.23:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.24:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.25:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.21:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.22:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.23:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.24:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.25:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→