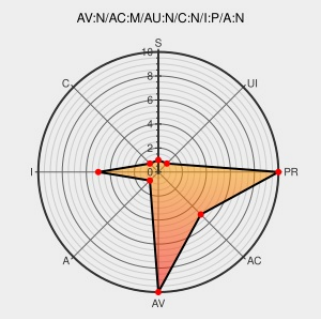
CVE-2011-1398

Published on: 08/30/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1398

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



Certain versions of Php from Php contain the following vulnerability:

The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

CVE-2011-1398 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
article.gmane.org | 522: Connection timed out	article.gmane.org text/html Inactive Link Not Archived	MLIST [internals] 20120203 [PHP-DEV] The case of HTTP response splitting protection in PHP
[security-announce] SUSE-SU-2013:1315-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2013:1315
oss-security - Re: php header() header injection detection bypass	openwall.com text/html	MLIST [oss-security] 20120905 Re: php header() header injection detection bypass
oss-security - php header() header injection detection bypass	openwall.com text/html	MLIST [oss-security] 20120829 php header() header injection detection bypass

About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 55078
PHP :: Bug #60227 :: header() cannot detect the multi-line header with CR(0x0D).	bugs.php.net text/xml	MISC bugs.php.net/bug.php?id=60227
PHP HTTP Response Splitting Header Injection Protection Can Be Bypassed Using Carriage Return Characters - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1027463
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1307
CVE-2011-1398	security-tracker.debian.org text/html	CONFIRM security-tracker.debian.org/tracker/CVE-2011-1398
USN-1569-1: PHP vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1569-1

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	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	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	5.3.2	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:5.3.0:*:*:*:*:*:*:*:

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

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

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:5.3.2:*:*:*:*:*:*:*:

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→

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