

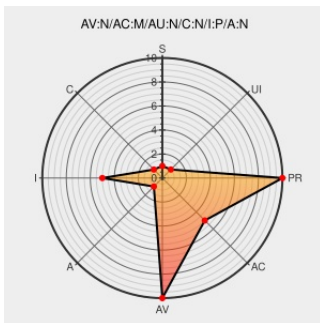


CVE-2011-1398

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 [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

article.gmane.org | 522: Connection timed out

[article.gmane.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[S](#) 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 hvnass

About Secunia Research Flexera	secunia.com Deprecated 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	 SECTRAK 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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](#) 2023   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)