CVE-2012-4388

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-4388
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-07 22:55:00 UTC
Updated	2023-11-07 02:11:00 UTC
Description	The sapi_header_op function in main/SAPI.c in PHP 5.4.0RC2 through 5.4.0 does not properly determine a pointer during c

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.0	rc2	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.0	rc2	All	All

References

Reference	Source
article.gmane.org | 522: Connection timed out	MLIST
oss-security - Re: Re: php header() header injection detection bypass	MLIST
CVE-2012-4388	CONFIR

[security-announce] SUSE-SU-2013:1315-1: important: Security update for	SUSE
oss-security - Re: php header() header injection detection bypass	MLIST
oss-security - Re: php header() header injection detection bypass	MLIST
oss-security - php header() header injection detection bypass	MLIST
PHP :: Bug #60227 :: header() cannot detect the multi-line header with CR(0x0D).	MISC
PHP HTTP Response Splitting Header Injection Protection Can Be Bypassed Using Carriage Return Characters - SecurityTracker	SECTRA
USN-1569-1: PHP vulnerabilities | Ubuntu	UBUNTU
PHP: Diff of /php/php-src/branches/PHP_5_4/main/SAPI.c	CONFIR
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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