



CVE-2017-11142

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

Summary

CVE	CVE-2017-11142
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-10 14:29:00 UTC
Updated	2018-01-14 02:29:00 UTC
Description	In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service by sending a crafted request to the server.

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All

Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All
Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	All	All	All	All

References				
Reference	Source	Link		
Fix bug #73807 · php/php-src@a15bffd · GitHub	CONFIRM	github		
oss-security - Re: CVE IDs needed for PHP vulnerabilities (affects 5.6.30 and 7.0.20)	CONFIRM	opensuse		
PHP: PHP 7 ChangeLog	CONFIRM	php.net		
Fix bug #73807 · php/php-src@0f8cf3b · GitHub	CONFIRM	github		
Malformed Request	BID	www.bids.com		
Debian -- Security Information -- DSA-4081-1 php5	DEBIAN	www.debian.org		
[R1] SecurityCenter 5.3.2, 5.4.0, 5.4.2, 5.4.5, 5.5.0, and 5.5.1 Fixes Multiple Vulnerabilities - Security Advisory Tenable™	CONFIRM	www.tenable.com		
PHP :: Sec Bug #73807 :: Performance problem with processing post request over 2000000 chars	CONFIRM	bugzilla		
PHP: PHP 5.6.30, 7.0.20, 7.1.2	CONFIRM	php.net		

PHP: PHP 5 ChangeLog	CONFIRM	php
September 2017 PHP Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	sec
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API [cve.report/api](#)

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