



CVE-2016-6290

Published on: 07/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-6290

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Php](#) from [Php](#) contain the following vulnerability: ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

CVE-2016-6290 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
About the security content of macOS Sierra 10.12 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT207170
PHP :: Sec Bug #72562 :: Use After Free in unserialize() with Unexpected	Issue Tracking bugs.php.net	CONFIRM bugs.php.net/72562

Session Deserialization	text/html	
PHP 'session.c' Use After Free Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 92097
PHP: PHP 7 ChangeLog	php.net text/html	 CONFIRM php.net/ChangeLog-7.php
APPLE-SA-2016-09-20 macOS Sierra 10.12	lists.apple.com text/html	 APPLE APPLE-SA-2016-09-20
208.43.231.11 Git - php-src.git/commit	Exploit Issue Tracking Mitigation git.php.net text/xml	 CONFIRM git.php.net/?p=php-src.git;a=commit;h=3798eb6fd5dddb211b01d41495072fd9858d4e32
Debian -- Security Information -- DSA-3631-1 php5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3631
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2750
PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1036430
PHP: PHP 5 ChangeLog	Release Notes php.net text/html	 CONFIRM php.net/ChangeLog-5.php
oss-security - Re: Fwd: CVE for PHP 5.5.38 issues	Mailing List Release Notes openwall.com text/html	 MLIST [oss-security] 20160724 Re: Fwd: CVE for PHP 5.5.38 issues
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201611-22

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	5.6.0	alpha1	All	All
Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All

Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.23	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	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	7.0.8	All	All	All
Application	Php	Php	5.6.0	alpha1	All	All

Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.23	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	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	7.0.8	All	All	All
Application	Php	Php	All	All	All	All
cpe:2.3:a:php:php:5.6.0:alpha1:*****:						
cpe:2.3:a:php:php:5.6.0:alpha2:*****:						
cpe:2.3:a:php:php:5.6.0:alpha3:*****:						
cpe:2.3:a:php:php:5.6.0:alpha4:*****:						
cpe:2.3:a:php:php:5.6.0:alpha5:*****:						
cpe:2.3:a:php:php:5.6.0:beta1:*****:						
cpe:2.3:a:php:php:5.6.0:beta2:*****:						
cpe:2.3:a:php:php:5.6.0:beta3:*****:						
cpe:2.3:a:php:php:5.6.0:beta4:*****:						
cpe:2.3:a:php:php:5.6.1:*****:						
cpe:2.3:a:php:php:5.6.10:*****:						
cpe:2.3:a:php:php:5.6.11:*****:						
cpe:2.3:a:php:php:5.6.12:*****:						
cpe:2.3:a:php:php:5.6.13:*****:						
cpe:2.3:a:php:php:5.6.14:*****:						
cpe:2.3:a:php:php:5.6.15:*****:						
cpe:2.3:a:php:php:5.6.16:*****:						
cpe:2.3:a:php:php:5.6.17:*****:						
cpe:2.3:a:php:php:5.6.18:*****:						
cpe:2.3:a:php:php:5.6.19:*****:						
cpe:2.3:a:php:php:5.6.2:*****:						
cpe:2.3:a:php:php:5.6.20:*****:						
cpe:2.3:a:php:php:5.6.21:*****:						
cpe:2.3:a:php:php:5.6.22:*****:						
cpe:2.3:a:php:php:5.6.23:*****:						
cpe:2.3:a:php:php:5.6.3:*****:						

cpe:2.3:a:php:php:5.6.4:*****:
cpe:2.3:a:php:php:5.6.5:*****:
cpe:2.3:a:php:php:5.6.6:*****:
cpe:2.3:a:php:php:5.6.7:*****:
cpe:2.3:a:php:php:5.6.8:*****:
cpe:2.3:a:php:php:5.6.9:*****:
cpe:2.3:a:php:php:7.0.0:*****:
cpe:2.3:a:php:php:7.0.1:*****:
cpe:2.3:a:php:php:7.0.2:*****:
cpe:2.3:a:php:php:7.0.3:*****:
cpe:2.3:a:php:php:7.0.4:*****:
cpe:2.3:a:php:php:7.0.5:*****:
cpe:2.3:a:php:php:7.0.8:*****:
cpe:2.3:a:php:php:5.6.0:alpha1:*****:
cpe:2.3:a:php:php:5.6.0:alpha2:*****:
cpe:2.3:a:php:php:5.6.0:alpha3:*****:
cpe:2.3:a:php:php:5.6.0:alpha4:*****:
cpe:2.3:a:php:php:5.6.0:alpha5:*****:
cpe:2.3:a:php:php:5.6.0:beta1:*****:
cpe:2.3:a:php:php:5.6.0:beta2:*****:
cpe:2.3:a:php:php:5.6.0:beta3:*****:
cpe:2.3:a:php:php:5.6.0:beta4:*****:
cpe:2.3:a:php:php:5.6.1:*****:
cpe:2.3:a:php:php:5.6.10:*****:
cpe:2.3:a:php:php:5.6.11:*****:
cpe:2.3:a:php:php:5.6.12:*****:
cpe:2.3:a:php:php:5.6.13:*****:
cpe:2.3:a:php:php:5.6.14:*****:

cpe:2.3:a:php:php:5.6.15:*****:
cpe:2.3:a:php:php:5.6.16:*****:
cpe:2.3:a:php:php:5.6.17:*****:
cpe:2.3:a:php:php:5.6.18:*****:
cpe:2.3:a:php:php:5.6.19:*****:
cpe:2.3:a:php:php:5.6.2:*****:
cpe:2.3:a:php:php:5.6.20:*****:
cpe:2.3:a:php:php:5.6.21:*****:
cpe:2.3:a:php:php:5.6.22:*****:
cpe:2.3:a:php:php:5.6.23:*****:
cpe:2.3:a:php:php:5.6.3:*****:
cpe:2.3:a:php:php:5.6.4:*****:
cpe:2.3:a:php:php:5.6.5:*****:
cpe:2.3:a:php:php:5.6.6:*****:
cpe:2.3:a:php:php:5.6.7:*****:
cpe:2.3:a:php:php:5.6.8:*****:
cpe:2.3:a:php:php:5.6.9:*****:
cpe:2.3:a:php:php:7.0.0:*****:
cpe:2.3:a:php:php:7.0.1:*****:
cpe:2.3:a:php:php:7.0.2:*****:
cpe:2.3:a:php:php:7.0.3:*****:
cpe:2.3:a:php:php:7.0.4:*****:
cpe:2.3:a:php:php:7.0.5:*****:
cpe:2.3:a:php:php:7.0.8:*****:
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](#)