



# CVE-2019-9024

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

## Summary

<b>CVE</b>	CVE-2019-9024
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-22 23:29:00 UTC
<b>Updated</b>	2019-06-18 18:15:00 UTC
<b>Description</b>	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decod

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

## References

Reference	Source	Link	Tags
-----------	--------	------	------

[security-announce] openSUSE-SU-2019:1256-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
February 2019 PHP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party Advise
Debian -- Security Information -- DSA-4398-1 php7.0	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advise
[security-announce] openSUSE-SU-2019:1572-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
USN-3902-2: PHP vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advise
PHP Information Disclosure and Heap Buffer Overflow Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advise
USN-3902-1: PHP vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advise
[security-announce] openSUSE-SU-2019:1293-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third
[security-announce] openSUSE-SU-2019:1573-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
PHP :: Sec Bug #77380 :: Global out of bounds read in xmlrpc base64 code	MISC	<a href="https://bugs.php.net">bugs.php.net</a>	Exploit, Issue Trac
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysi

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159670](#) Oracle Enterprise Linux Security Update for php:7.2 (ELSA-2020-1624)
- [296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)
- [377294](#) Alibaba Cloud Linux Security Update for Hypertext Preprocessor (PHP) (ALINUX2-SA-2020:0054)
- [501126](#) Alpine Linux Security Update for php7
- [752878](#) SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4067-1)
- [940404](#) AlmaLinux Security Update for php:7.2 (ALSA-2020:1624)
- [960218](#) Rocky Linux Security Update for php:7.2 (RLSA-2020:1624)

© 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](#).

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