



# CVE-2022-31626

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

## Summary

<b>CVE</b>	CVE-2022-31626
<b>State</b>	PUBLIC
<b>Assigner</b>	security@php.net
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-16 06:15:00 UTC
<b>Updated</b>	2023-11-07 03:47:00 UTC
<b>Description</b>	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd dri

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	All	All	All	All

## References

Reference	Source	Link	Tags
PHP: Multiple Vulnerabilities (GLSA 202209-20) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
July 2022 PHP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
PHP :: Sec Bug #81719 :: mysqlnd/pdo password buffer overflow leading to RCE	MISC	<a href="https://bugs.php.net">bugs.php.net</a>	
[SECURITY] Fedora 36 Update: php-8.1.7-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Debian -- Security Information -- DSA-5179-1 php7.4	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 36 Update: php-8.1.7-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: php-8.0.20-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: php-8.0.20-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 3243-1] php7.3 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** c dot fol at ambionics dot io

## Legacy QID Mappings

150542	PHP Multiple Remote Code Execution Vulnerabilities (CVE-2022-31626,CVE-2022-31625)
159966	Oracle Enterprise Linux Security Update for php:8.0 (ELSA-2022-5468)
159968	Oracle Enterprise Linux Security Update for php:7.4 (ELSA-2022-5467)
160021	Oracle Enterprise Linux Security Update for Hypertext Preprocessor (PHP) (ELSA-2022-5904)
180815	Debian Security Update for php7.4 (DSA 5179-1)
181332	Debian Security Update for php7.3 (DLA 3243-1)
198831	Ubuntu Security Notification for Hypertext Preprocessor (PHP) Vulnerabilities (USN-5479-1)
240509	Red Hat Update for php:7.4 (RHSA-2022:5467)
240510	Red Hat Update for php:8.0 (RHSA-2022:5468)
240514	Red Hat Update for php:7.4 (RHSA-2022:5471)
240535	Red Hat Update for rh-php73-php (RHSA-2022:5491)
240592	Red Hat Update for Hypertext Preprocessor (PHP) (RHSA-2022:5904)
282833	Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-f3fc52428e)
282834	Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-0a96e5b9b1)
296084	Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)
356076	Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-006
356087	Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-006
377131	Alibaba Cloud Linux Security Update for php:7.4 (ALINUX3-SA-2022:0147)
38872	Multiple Vulnerabilities in Hypertext Preprocessor (PHP)
38883	Hypertext Preprocessor (PHP) Multiple Security Vulnerabilities (81719, 81720)
502333	Alpine Linux Security Update for php81
502516	Alpine Linux Security Update for php7
502517	Alpine Linux Security Update for php8

502567	Alpine Linux Security Update for php/
502574	Alpine Linux Security Update for php8
502912	Alpine Linux Security Update for php81
503680	Alpine Linux Security Update for php8
505791	Alpine Linux Security Update for php81
672018	EulerOS Security Update for Hypertext Preprocessor (PHP) (EulerOS-SA-2022-2229)
710633	Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 202209-20)
752263	SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2022:2161-1)
752270	SUSE Enterprise Linux Security Update for php72 (SUSE-SU-2022:2183-1)
752271	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:2185-1)
752289	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:2275-1)
752863	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:3997-1)
752878	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4067-1)
752898	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4069-1)
752901	SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2022:4068-1)
753278	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:2292-1)
753350	SUSE Enterprise Linux Security Update for php8 (SUSE-SU-2022:2303-1)
902353	Common Base Linux Mariner (CBL-Mariner) Security Update for Hypertext Preprocessor (PHP) (9944)
940617	AlmaLinux Security Update for Hypertext Preprocessor (PHP) (ALSA-2022:5904)
940651	AlmaLinux Security Update for php:8.0 (ALSA-2022:5468)
960146	Rocky Linux Security Update for php:8.0 (RLSA-2022:5468)
960154	Rocky Linux Security Update for php:7.4 (RLSA-2022:5467)
960523	Rocky Linux Security Update for Hypertext Preprocessor (PHP) (RLSA-2022:5904)

© [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](#)