



CVE-2022-31631

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

Summary

CVE	CVE-2022-31631
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	Unknown
Updated	2022-05-25 22:10:45 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160478](#) Oracle Enterprise Linux Security Update for php:8.0 (ELSA-2023-0848)

[160486](#) Oracle Enterprise Linux Security Update for Hypertext Preprocessor (PHP) (ELSA-2023-0965)

[160592](#) Oracle Enterprise Linux Security Update for 8.1 (ELSA-2023-2417)

[160672](#) Oracle Enterprise Linux Security Update for php:7.4 (ELSA-2023-2903)

[181613](#) Debian Security Update for php7.3 (DLA 3345-1)

[181663](#) Debian Security Update for php7.4 (DSA 5363-1)

[182937](#) Debian Security Update for php8.2 (CVE-2022-31631)

[199126](#) Ubuntu Security Notification for Hypertext Preprocessor (PHP) Vulnerability (USN-5818-1)

[199545](#) Ubuntu Security Notification for Hypertext Preprocessor (PHP) Vulnerabilities (USN-5905-1)

[241205](#) Red Hat Update for php:8.0 (RHSA-2023:0848)

241219 Red Hat Update for Hypertext Preprocessor (PHP) (RHSA-2023:0965)
241447 Red Hat Update for php:8.1 (RHSA-2023:2417)
241540 Red Hat Update for php:7.4 (RHSA-2023:2903)
283603 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2023-2dc2d607ba)
283613 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2023-5732365005)
355222 Amazon Linux Security Advisory for php8.1 : ALAS2023-2023-081
356063 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-003
356086 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-003
356088 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.1-2023-003
356281 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALAS2PHP8.2-2023-003
378747 Alibaba Cloud Linux Security Update for php:7.4 (ALINUX3-SA-2023:0088)
502622 Alpine Linux Security Update for php8
502623 Alpine Linux Security Update for php81
503214 Alpine Linux Security Update for php82
506154 Alpine Linux Security Update for php82
672862 EulerOS Security Update for Hypertext Preprocessor (PHP) (EulerOS-SA-2023-1603)
753501 SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2023:0072-1)
753504 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2023:0084-1)
753508 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2023:0073-1)
753531 SUSE Enterprise Linux Security Update for php8 (SUSE-SU-2023:0074-1)
753778 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2023:0476-1)
940930 AlmaLinux Security Update for php:8.0 (ALSA-2023:0848)
940947 AlmaLinux Security Update for Hypertext Preprocessor (PHP) (ALSA-2023:0965)
941025 AlmaLinux Security Update for php:8.1 (ALSA-2023:2417)
941091 AlmaLinux Security Update for php:7.4 (ALSA-2023:2903)
960657 Rocky Linux Security Update for php:8.0 (RLSA-2023:0848)
960904 Rocky Linux Security Update for Hypertext Preprocessor (PHP) (RLSA-2023:0965)

© [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](#)