



CVE-2021-21704

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

Summary

CVE	CVE-2021-21704
State	PUBLIC
Assigner	security@php.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-04 04:15:00 UTC
Updated	2022-10-25 14:58:00 UTC
Description	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Php	Php	All	All	All	All

References

Reference	Source	Link	Tags
PHP: Multiple Vulnerabilities (GLSA 202209-20) — Gentoo security	GENTOO	security.gentoo.org	
PHP :: Sec Bug #76450 :: SIGSEGV in firebird_stmt_execute	CONFIRM	bugs.php.net	
PHP :: Sec Bug #76452 :: Crash while parsing blob data in firebird_fetch_blob	CONFIRM	bugs.php.net	
PHP :: Sec Bug #76449 :: SIGSEGV in firebird_handle_doer	CONFIRM	bugs.php.net	
PHP :: Sec Bug #76448 :: Stack buffer overflow in firebird_info_cb	CONFIRM	bugs.php.net	
September 2021 PHP Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: reported by trichimtrich at gmail dot com

Legacy QID Mappings

150469	PHP Multiple Vulnerabilities (CVE-2021-21704,CVE-2021-21705)
178696	Debian Security Update for php7.3 (DSA 4935-1)
178707	Debian Security Update for php7.0 (DLA 2708-1)
179882	Debian Security Update for php7.4 (CVE-2021-21704)
198429	Ubuntu Security Notification for Hypertext Preprocessor vulnerabilities (USN-5006-1)
281697	Fedora Security Update for php (FEDORA-2021-d867b595d1)
281698	Fedora Security Update for php (FEDORA-2021-172c8bd11d)
352803	Amazon Linux Security Advisory for php73: ALAS-2021-1532
356070	Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-008
356080	Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-008
38844	PHP Multiple Security Vulnerabilities
670721	EulerOS Security Update for php (EulerOS-SA-2021-2479)
710633	Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 202209-20)
750933	SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2021:2636-1)
750936	SUSE Enterprise Linux Security Update for php72 (SUSE-SU-2021:2638-1)
750937	OpenSUSE Security Update for php7 (openSUSE-SU-2021:2637-1)
750952	OpenSUSE Security Update for php7 (openSUSE-SU-2021:1130-1)
750991	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2021:2795-1)
751019	OpenSUSE Security Update for php7 (openSUSE-SU-2021:2795-1)
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)
901082	Common Base Linux Mariner (CBL-Mariner) Security Update for Hypertext Preprocessor (PHP) (7326)

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](#)