



CVE-2019-11831

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-11831
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-09 04:29:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	The PharStreamWrapper (aka phar-stream-wrapper) package 2.x before 2.1.1 and 3.x before 3.1.1 for TYPO3 does not pre

Risk And Classification

Problem Types: CWE-22 | CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Drupal	Drupal	All	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Joomla	Joomla!	All	All	All	All
Application	Typo3	Pharstreamwrapper	All	All	All	All
Application	Typo3	Pharstreamwrapper	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 29 Update: drupal7-7.67-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists
By-passing protection of Phar Stream Wrapper Interceptor	MISC	typo
TYPO3 PharStreamWrapper Package CVE-2019-11831 Directory Traversal Vulnerability	BID	www
[SECURITY] Fedora 28 Update: drupal7-7.67-1.fc28 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 29 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc29 - package-announce - Fedora Mailing-Lists		lists

[SECURITY] Fedora 28 Update: drupal7-7.67-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] [DLA 1797-1] drupal7 security update	MLIST	lists
[SECURITY] Fedora 28 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc28 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 29 Update: drupal7-7.67-1.fc29 - package-announce - Fedora Mailing-Lists		lists
Bugtraq: [SECURITY] [DSA 4445-1] drupal7 security update	BUGTRAQ	secl
[SECURITY] Fedora 29 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] Fedora 30 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc30 - package-announce - Fedora Mailing-Lists		lists
Drupal core - Moderately critical - Third-party libraries - SA-CORE-2019-007 Drupal.org	CONFIRM	www
Release Phar Alias Handling & Performance · TYPO3/phar-stream-wrapper · GitHub	MISC	githu
[SECURITY] Fedora 30 Update: drupal7-7.67-1.fc30 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 30 Update: drupal7-7.67-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Release Phar Alias Handling & Performance · TYPO3/phar-stream-wrapper · GitHub	MISC	githu
[SECURITY] Fedora 28 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Debian -- Security Information -- DSA-4445-1 drupal7	DEBIAN	www
[SECURITY] Fedora 30 Update: php-typo3-phar-stream-wrapper-3.1.1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Synology Inc.	CONFIRM	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)