



CVE-2018-12015

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

Summary

CVE	CVE-2018-12015
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-07 13:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In Perl through 5.26.2, the Archive::Tar module allows remote attackers to bypass a directory-traversal protection mechanism.

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Archive		tar_project	archive		tar
Application	Archive		tar_project	archive\	\	tar
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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snap Creator Framework	-	All	All	All
Application	Netapp	Snap Creator Framework	-	All	All	All
Application	Perl	Perl	All	All	All	All

References

Reference

Full Disclosure: APPLE-SA-2019-3-25-2 macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra

Oracle Critical Patch Update Advisory - July 2020

#900834 - perl: CVE-2018-12015: Archive::Tar: directory traversal - Debian Bug report logs

Debian -- Security Information -- DSA-4226-1 perl

USN-3684-1: Perl vulnerability | Ubuntu security notices

USN-3684-2: Perl vulnerability | Ubuntu security notices

CVE-2018-12015 Perl Vulnerability in NetApp Products | NetApp Product Security

Perl CVE-2018-12015 Directory Traversal Vulnerability

About the security content of macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra - Apple Support

Bugtraq: APPLE-SA-2019-3-25-2 macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra

Perl Directory Traversal Flaw in Archive::Tar Lets Remote Users Overwrite Files on the Target System - SecurityTracker

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296091](#) Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)

[377525](#) Alibaba Cloud Linux Security Update for perl-archive-tar (ALINUX2-SA-2019:0088)

[500524](#) Alpine Linux Security Update for perl

[504285](#) Alpine Linux Security Update for perl

© [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](#)