



CVE-2018-18312

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

Summary

CVE	CVE-2018-18312
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-05 22:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Snapcenter	-	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
Application	Perl	Perl	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All

References

Reference

Bug #133423 for perl5: [CVE-2018-18312] regcomp: heap-buffer-overflow write / reg_node overrun (perl-5.28.0, 5.26.2)

Oracle Critical Patch Update Advisory - July 2020

Perl: Multiple vulnerabilities (GLSA 201909-01) — Gentoo security

1646734 – (CVE-2018-18312) CVE-2018-18312 perl: Heap-based buffer overflow in S_handle_regex_sets()

Debian -- Security Information -- DSA-4347-1 perl

perldelta - what is new for perl v5.28.1 - metacpan.org

[SECURITY] Fedora 29 Update: perl-5.28.1-425.fc29 - package-announce - Fedora Mailing-Lists

December 2018 PERL Vulnerabilities in NetApp Products | NetApp Product Security

perldelta - what is new for perl v5.26.3 - metacpan.org

Red Hat Customer Portal

[SECURITY] Fedora 29 Update: perl-5.28.1-425.fc29 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

Perl CVE-2018-18312 Heap Buffer Overflow Vulnerability

Perl Function Integer/Heap Overflows Let Local Users Obtain Potentially Sensitive Information or Remote Users Execute Arbitrary Code in Ce

USN-3834-1: Perl vulnerabilities | Ubuntu security notices

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296087 Oracle Solaris 11.4 Support Repository Update (SRU) 8.1.5 Missing (CPUAPR2019)

500525 Alpine Linux Security Update for perl

504286 Alpine Linux Security Update for perl

710131 Gentoo Linux Perl Multiple vulnerabilities (GLSA 201909-01)

© [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](#)