



CVE-2019-20454

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

Summary

CVE	CVE-2019-20454
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-14 14:15:00 UTC
Updated	2024-03-27 16:05:00 UTC
Description	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern \X is JIT compiled and used to match speci

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Pcre	Pcre2	All	All	All	All
Application	Pcre	Pcre2	All	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 31 Update: mingw-pcre2-10.33-3.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
1735494 – (CVE-2019-20454) CVE-2019-20454 pcre: Out of bounds read in JIT mode when \X is used in non-UTF mode	MISC	bugzilla.redhat.com
Bug 2421 – Array cross-border reading/global variable coverage in PCRE Library	MISC	bugzilla.redhat.com
[SECURITY] [DLA 3363-1] pcre2 security update	MLIST	lists.fedoraproject.org
PHP :: Sec Bug #78338 :: Array cross-border reading/global variable coverage in PCRE	MISC	bugzilla.redhat.com
[pcre2] Revision 1092	MISC	vcs.pcre.org
[SECURITY] Fedora 31 Update: mingw-pcre2-10.33-3.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
PCRE2: Denial of service (GLSA 202006-16) — Gentoo security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181631](#) Debian Security Update for pcre2 (DLA 3363-1)

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[377374](#) Alibaba Cloud Linux Security Update for pcre2 security and enhancement update (moderate) (ALINUX3-SA-2022:0050)

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[752435](#) SUSE Enterprise Linux Security Update for pcre2 (SUSE-SU-2022:2649-1)

[770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

[940227](#) AlmaLinux Security Update for pcre2 (ALSA-2020:4539)

[940250](#) AlmaLinux Security Update for php:7.3 (ALSA-2020:3662)

[960390](#) Rocky Linux Security Update for pcre2 (RLSA-2020:4539)

[960421](#) Rocky Linux Security Update for php:7.3 (RLSA-2020:3662)

© [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](#)