CVE-2019-20387

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-20387
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-21 23:15:00 UTC
Updated	2023-01-31 20:49:00 UTC
Description	repodata_schema2id in repodata.c in libsolv before 0.7.6 has a heap-based buffer over-read via a last schema whose lengt

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Opensuse	Libsolv	All	All	All	All
Application	Opensuse	Libsolv	All	All	All	All

References

Reference	Source	Link	Tags
Comparing 0.7.5...0.7.6 · openSUSE/libsolv · GitHub	MISC	github.com	Patch, Thi
[SECURITY] [DLA 2088-1] libsolv security update	MLIST	lists.debian.org	
repodata_schema2id: fix heap-buffer-overflow in memcmp · openSUSE/libsolv@fdb9c9c · GitHub	MISC	github.com	Patch, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

750732 SUSE Enterprise Linux Security Update for libsolv (SUSE-SU-2021:2180-1)

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

940306 AlmaLinux Security Update for libsolv (ALSA-2020:4508)

© 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 registred 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