



CVE-2021-44571

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-44571
State	REJECT
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-21 20:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplic

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Opensuse	Libsolv	All	All	All	All
Application	Opensuse	Libsolv	All	All	All	All

References

Reference	Source	Link
libsolv "prefer_suggested" function a heap overflow vulnerability · Issue #421 · openSUSE/libsolv · GitHub	MISC	github.com
[SECURITY] Fedora 35 Update: libsolv-0.7.21-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
PoC/PoC-prefer_suggested-442 at master · yangjiageng/PoC · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[282447](#) Fedora Security Update for libsolv (FEDORA-2022-f8921a3891)

[900699](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsolv (8729)

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)