



CVE-2020-8032

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

Summary

CVE	CVE-2020-8032
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-25 10:15:00 UTC
Updated	2021-03-03 15:41:00 UTC
Description	A Insecure Temporary File vulnerability in the packaging of cyrus-sasl of openSUSE Factory allows local attackers to escalate

Risk And Classification

Problem Types: CWE-377

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensuse	Cyrus-sasl	All	All	All	All

References

Reference	Source	Link
Bug 1180669 – VUL-0: CVE-2020-8032: cyrus-sasl: Local privilege escalation to root due to insecure tmp file usage	CONFIRM	bugzilla.su
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

LEGACY: Johannes Segitz of SUSE

Legacy QID Mappings

[900126](#) CBL-Mariner Linux Security Update for cyrus-sasl 2.1.27

[901591](#) Common Base Linux Mariner (CBL-Mariner) Security Update for cyrus-sasl (6370-1)

[902801](#) Common Base Linux Mariner (CBL-Mariner) Security Update for cyrus-sasl (3914)

© [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](#)