



CVE-2022-31256

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

Summary

CVE	CVE-2022-31256
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-26 09:15:00 UTC
Updated	2022-10-28 17:49:00 UTC
Description	A Improper Link Resolution Before File Access ('Link Following') vulnerability in a script called by the sendmail systemd ser

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensuse	Factory	All	All	All	All

References

Reference	Source	Link
Bug 1204696 – VUL-0: CVE-2022-31256: sendmail: mail to root privilege escalation via sm-client.pre script	CONFIRM	bugzilla.suse.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Matthias Gerstner and Filippo Bonazzi from SUSE

Legacy QID Mappings

[752770](#) SUSE Enterprise Linux Security Update for sendmail (SUSE-SU-2022:3899-1)

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](#)