



CVE-2021-25316

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

Summary

CVE	CVE-2021-25316
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-14 10:15:00 UTC
Updated	2023-04-14 18:50:00 UTC
Description	A Insecure Temporary File vulnerability in s390-tools of SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Ser

Risk And Classification

Problem Types: CWE-377

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Suse	Linux Enterprise Server	15	sp2	All	All
Operating System	Suse	Linux Enterprise Server	15	sp5	All	All
Application	Suse	S390-tools	All	All	All	All

References

Reference	Source
Bug 1182777 – VUL-0: CVE-2021-25316: s390-tools: Local DoS of VM live migration due to use of static tmp files in detach_disks.sh	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Wolfgang Frisch of SUSE

Legacy QID Mappings

[174798](#) SUSE Enterprise Linux Security update for s390-tools (SUSE-SU-2021:0777-1)

© [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](#)