



CVE-2019-3687

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

Summary

CVE	CVE-2019-3687
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-24 09:15:00 UTC
Updated	2020-03-05 01:15:00 UTC
Description	The permission package in SUSE Linux Enterprise Server allowed all local users to run dumpcap in the "easy" permission p

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Suse	Linux Enterprise Server	-	All	All	All
Operating System	Suse	Linux Enterprise Server	-	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2020:0302-1: moderate: Security update f	SUSE
Bug 1148788 – VUL-0: CVE-2019-3687: permissions: easy profile allows everyone execute dumpcap and read all network traffic	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Malte Kraus of SUSE

Legacy QID Mappings

[751472](#) OpenSUSE Security Update for permissions (openSUSE-SU-2021:1520-1)

© [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](#)