



CVE-2018-17953

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

Summary

CVE	CVE-2018-17953
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-27 13:29:00 UTC
Updated	2023-11-07 02:54:00 UTC
Description	A incorrect variable in a SUSE specific patch for pam_access rule matching in PAM 1.3.0 in openSUSE Leap 15.0 and SUSE Linux Enterprise Server 15 SP3

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kernel	Linux-pam	1.3.0	All	All	All
Application	Kernel	Linux-pam	1.3.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Suse	Linux Enterprise	15.0	All	All	All
Operating System	Suse	Linux Enterprise	15.0	All	All	All

References

Reference

- Bug 1115640 – VUL-0: CVE-2018-17953: pam: (at least /lib64/security/pam_access.so) doesn't properly handle with ip addresses and subnet
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Daniel Pecka

There are currently no legacy QID mappings associated with this CVE.

© [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](#)