



CVE-2020-27780

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

Summary

CVE	CVE-2020-27780
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-18 00:15:00 UTC
Updated	2020-12-28 19:11:00 UTC
Description	A flaw was found in Linux-Pam in versions prior to 1.5.1 in the way it handle empty passwords for non-existing users. When

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-pam	Linux-pam	All	All	All	All
Application	Linux-pam	Linux-pam	All	All	All	All

References

Reference	Source
1901094 – (CVE-2020-27780) CVE-2020-27780 pam: authentication bypass when the user doesn't exist and root password is blank	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501427 Alpine Linux Security Update for linux-pam
501749 Alpine Linux Security Update for linux-pam
504123 Alpine Linux Security Update for linux-pam
900022 CBL-Mariner Linux Security Update for pam 1.3.1

© [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](#)