CVE-2022-0022

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0022
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-09 18:15:00 UTC
Updated	2022-03-12 02:31:00 UTC
Description	Usage of a weak cryptographic algorithm in Palo Alto Networks PAN-OS software where the password hashes of administr

Risk And Classification

Problem Types: CWE-916

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

References

Reference	Source	Link
CVE-2022-0022 PAN-OS: Use of a Weak Cryptographic Algorithm for Stored Password Hashes	CONFIRM	security.paloaltonetworks.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks an external security researcher for discovering and reporting this issue.

Legacy QID Mappings

730391 Palo Alto Networks (PAN-OS) Use of a Weak Cryptographic Algorithm for Stored Password Hashes Vulnerability (PAN-127479)