CVE-2022-0030

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0030
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-12 17:15:00 UTC
Updated	2022-10-14 15:33:00 UTC
Description	An authentication bypass vulnerability in the Palo Alto Networks PAN-OS 8.1 web interface allows a network-based attacke

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
CVE-2022-0030 PAN-OS: Authentication Bypass in Web Interface	MISC	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks the security researcher that discovered and reported this issue.

Legacy QID Mappings

730624 Palo Alto Networks (PAN-OS) Authentication Bypass Vulnerability in Web Interface (PAN-195571)

© 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 registred 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