PAN-OS: Unauthenticated user initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0300
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 19:16:35 UTC
Updated	2026-05-07 17:46:44 UTC
Description	A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:M/U:Red

EPSS: 0.148970000 probability, percentile 0.945690000 (date 2026-05-07)

CISA KEV: Listed on 2026-05-06; due 2026-05-09; ransomware use Unknown

Problem Types: CWE-787 | CWE-787 CWE-787: Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:M/U:Red

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Palo Alto Networks
Product	PAN-OS
Name	Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. Until the vendor releases an official fix, the following workaround should be implemented: - Restrict User-ID Authentication Portal access to only trusted zones. - Disable User-ID Authentication Portal if not required.
Notes	https://security.paloaltonetworks.com/CVE-2026-0300 ; https://nvd.nist.gov/vuln/detail/CVE-2026-0300

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Paloaltonetworks	Pa-1410	-	All	All	All
Hardware	Paloaltonetworks	Pa-1420	-	All	All	All
Hardware	Paloaltonetworks	Pa-3410	-	All	All	All
Hardware	Paloaltonetworks	Pa-3420	-	All	All	All
Hardware	Paloaltonetworks	Pa-3430	-	All	All	All
Hardware	Paloaltonetworks	Pa-3440	-	All	All	All
Hardware	Paloaltonetworks	Pa-410	-	All	All	All
Hardware	Paloaltonetworks	Pa-410r	-	All	All	All
Hardware	Paloaltonetworks	Pa-410r-5g	-	All	All	All
Hardware	Paloaltonetworks	Pa-415	-	All	All	All
Hardware	Paloaltonetworks	Pa-415-5g	-	All	All	All
Hardware	Paloaltonetworks	Pa-440	-	All	All	All
Hardware	Paloaltonetworks	Pa-445	-	All	All	All
Hardware	Paloaltonetworks	Pa-450	-	All	All	All
Hardware	Paloaltonetworks	Pa-450r	-	All	All	All
Hardware	Paloaltonetworks	Pa-450r-5g	-	All	All	All
Hardware	Paloaltonetworks	Pa-455	-	All	All	All
Hardware	Paloaltonetworks	Pa-455-5g	-	All	All	All
Hardware	Paloaltonetworks	Pa-455r-5g	-	All	All	All
Hardware	Paloaltonetworks	Pa-460	-	All	All	All
Hardware	Paloaltonetworks	Pa-501	-	All	All	All
Hardware	Paloaltonetworks	Pa-505	-	All	All	All
Hardware	Paloaltonetworks	Pa-510	-	All	All	All
Hardware	Paloaltonetworks	Pa-520	-	All	All	All
Hardware	Paloaltonetworks	Pa-540	-	All	All	All
Hardware	Paloaltonetworks	Pa-5410	-	All	All	All

Hardware	Paloaltonetworks	Pa-5420	-	All	All	All
Hardware	Paloaltonetworks	Pa-5430	-	All	All	All
Hardware	Paloaltonetworks	Pa-5440	-	All	All	All
Hardware	Paloaltonetworks	Pa-5445	-	All	All	All
Hardware	Paloaltonetworks	Pa-545-poe	-	All	All	All
Hardware	Paloaltonetworks	Pa-5450	-	All	All	All
Hardware	Paloaltonetworks	Pa-550	-	All	All	All
Hardware	Paloaltonetworks	Pa-5540	-	All	All	All
Hardware	Paloaltonetworks	Pa-555-poe	-	All	All	All
Hardware	Paloaltonetworks	Pa-5550	-	All	All	All
Hardware	Paloaltonetworks	Pa-5560	-	All	All	All
Hardware	Paloaltonetworks	Pa-5570	-	All	All	All
Hardware	Paloaltonetworks	Pa-5580	-	All	All	All
Hardware	Paloaltonetworks	Pa-560	-	All	All	All
Hardware	Paloaltonetworks	Pa-7500	-	All	All	All
Hardware	Paloaltonetworks	Pa-7500-dpc-a	-	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.0	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h10	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h12	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h14	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h17	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h18	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h2	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h21	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h27	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h3	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h30	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h31	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h4	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h5	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h7	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.10	h9	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.11	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.12	All	All	All

Operating System	Paloaltonetworks	Pan-os	10.2.13	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h1	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h10	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h16	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h18	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h2	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h3	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h4	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h5	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.13	h7	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.14	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.15	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.16	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.16	h1	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.16	h4	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.16	h6	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.17	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.18	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.18	h1	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.18	h5	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.4	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.6	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	-	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h1	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h12	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h16	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h19	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h21	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h24	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h3	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h32	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.7	h6	All	All

Operating System	Paloaltonetworks	Pan-os	10.2.7	h8	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.8	All	All	All
Operating System	Paloaltonetworks	Pan-os	10.2.9	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.0	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h10	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h12	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h21	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h5	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h7	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.10	h9	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.11	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.12	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.13	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.13	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.13	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.13	h3	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.14	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h13	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h15	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h16	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h17	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h18	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h25	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h27	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h32	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.4	h7	All	All

Operating System	Paloaltonetworks	Pan-os	11.1.4	h9	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h10	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h14	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h17	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h19	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h20	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h21	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h22	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h23	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h25	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h29	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h3	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h5	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h6	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.6	h7	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.7	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.7	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.7	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.7	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.8	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.1.9	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.0	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	h3	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.10	h5	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.11	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.2	All	All	All

Operating System	Paloaltonetworks	Pan-os	11.2.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h10	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h11	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h12	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h14	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h15	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h5	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h6	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h7	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h8	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.4	h9	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.6	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	-	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h1	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h10	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h11	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h12	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h2	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h3	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h4	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h7	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.7	h8	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.8	All	All	All
Operating System	Paloaltonetworks	Pan-os	11.2.9	All	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.4	-	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.4	h2	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.4	h3	All	All
Operating System	Paloaltonetworks	Pan-os	12.1.5	-	All	All

Operating System	Paloaltonetworks	Pan-os	12.1.6	-	All	All
Hardware	Paloaltonetworks	Vm-100	-	All	All	All
Hardware	Paloaltonetworks	Vm-300	-	All	All	All
Hardware	Paloaltonetworks	Vm-50	-	All	All	All
Hardware	Paloaltonetworks	Vm-500	-	All	All	All
Hardware	Paloaltonetworks	Vm-700	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Cloud NGFW	unaffected All custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 12.1.0 12.1.7 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.15 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 10.2.0 10.2.18-h6 custom	Not specified
CNA	Palo Alto Networks	Prisma Access	unaffected All custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0300	psirt@paloaltonetworks.com	security.paloaltonetworks.com	Mitigatio
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Gove
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-05-06T17:27:00.000Z	Updated with Threat Prevention ID and clarified the Required Configuration section.
CNA	2026-05-05T23:00:00.000Z	Initial publication.
ADP	2026-05-06T00:00:00.000Z	CVE-2026-0300 added to CISA KEV

Solutions

CNA: This issue will be fixed in upcoming releases of PAN-OS as captured in the table above. We strongly recommend that you secure access to your User-ID™ Authentication Portal following the instructions in the workarounds section below.

Workarounds

CNA: Customers can mitigate the risk of this issue by taking either of the following actions: * Restrict User-ID™ Authentication Portal access to only trusted zones and in addition, disable Response Pages in the Interface Management Profile attached to every L3 interface in any zone where untrusted/internet traffic can ingress. Keep Response Pages enabled only on interfaces in trust/internal zones where legitimate users' browsers ingress. Refer to Step 6 of the following Live Community article (https://live.paloaltonetworks.com/t5/general-articles/why-it-s-essential-to-secure-your-management-interface/ta-p/1001286) and Knowledgebase article (https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CqbiCAC) for steps to restrict access. * Disable User-ID™ Authentication Portal if not required. Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510019 from Applications and Threats content version 9097-10022. Decoder capabilities necessitate PAN-OS 11.1 or a later version for Threat ID support.

Exploits

CNA: Limited exploitation has been observed targeting Palo Alto Networks User-ID™ Authentication Portals that are exposed to untrusted IP addresses and/or the public internet. Customers following standard security best practices, such as restricting sensitive portals to trusted internal networks are at a greatly reduced risk.

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