Autonomous Digital Experience Manager: Improper validation of ADEM certificate

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

Summary

CVE	CVE-2026-0233
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 08:16:22 UTC
Updated	2026-04-13 15:01:43 UTC
Description	A certificate validation vulnerability in Palo Alto Networks Autonomous Digital Experience Manager on Windows allows an u

Risk And Classification

Primary CVSS: v4.0 2 LOW from psirt@paloaltonetworks.com

CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/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:N/R:U/V:D/RE:M/U:Green

EPSS: 0.000100000 probability, percentile 0.011230000 (date 2026-04-15)

Problem Types: CWE-295 | CWE-295 CWE-295: Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	2	LOW	CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	2	LOW	CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/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:N/R:U/V:D/RE:M/U:Green

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Autonomous Digital Experience Manager	affected 5.10.0 5.10.14 custom	Windows

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0233	psirt@paloaltonetworks.com	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

CNA: David Fischer with OBI (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-08T16:00:00.000Z	Initial publication.
CNA	2026-04-08T18:05:00.000Z	Corrected the version ranges.

Solutions

CNA: Version Minor Version Suggested Solution Autonomous Digital Experience Manager 5.10 on Windows 5.10.0 through 5.10.14 Upgrade to 5.10.14 or later.

Workarounds

CNA: No known workarounds exist for this issue.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of this issue.

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