



# Autonomous Digital Experience Manager: Improper validation of ADEM certificate

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

## Summary

<b>CVE</b>	CVE-2026-0233
<b>State</b>	PUBLISHED
<b>Assigner</b>	palo_alto
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 08:16:22 UTC
<b>Updated</b>	2026-04-13 15:01:43 UTC
<b>Description</b>	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/MSX/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/MSX: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.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)