# Prisma SD-WAN: Improper Certificate Validation Vulnerability

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-0244 |
| **State** | PUBLISHED |
| **Assigner** | palo_alto |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-13 19:16:58 UTC |
| **Updated** | 2026-05-14 16:21:23 UTC |
| **Description** | An improper certificate validation vulnerability in the Palo Alto Networks Prisma SD-WAN ION enables man-in-the-middle (M |

## Risk And Classification

**Primary CVSS:** v4.0 5.2 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:A/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:Y/R:U/V:D/RE:M/U:Amber

**EPSS:** 0.000040000 probability, percentile 0.001600000 (date 2026-05-17)

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

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | psirt@paloaltonetworks.com | Secondary | 5.2 | MEDIUM | CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S |
| 4.0 | CNA | CVSS | 5.2 | MEDIUM | CVSS:4.0/AV:A/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

Adjacent

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:A/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:Y/R:U/V:D/RE:M/U:Amber

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Palo Alto Networks | Prisma SD-WAN ION | affected 6.5.0 6.5.3-b15 custom | Not specified |
| CNA | Palo Alto Networks | Prisma SD-WAN ION | affected 6.4.0 6.4.3-b8 custom | Not specified |
| CNA | Palo Alto Networks | Prisma SD-WAN ION | affected 6.3.0 6.3.6-b10 custom | Not specified |
| CNA | Palo Alto Networks | Prisma SD-WAN ION | unaffected 6.1.0 custom | Not specified |
| CNA | Palo Alto Networks | Prisma SD-WAN ION | unaffected 5.6.0 custom | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| security.paloaltonetworks.com/CVE-2026-0244 | 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:** Palo Alto Networks thanks our internal security research teams for discovering and reporting this issue. (en)

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| CNA | 2026-05-13T16:00:00.000Z | Initial publication. |

Solutions

**CNA:** Version Minor Version Suggested Solution Prisma SD-WAN ION 6.5 6.5.1 through 6.5.3 Upgrade to 6.5.3-b15 or later. Prisma SD-WAN ION 6.4 6.4.1 through 6.4.3 Upgrade to 6.4.3-b8 or later. Prisma SD-WAN ION 6.3 6.3.1 through 6.3.6 Upgrade to 6.3.6-b10 or later. Prisma SD-WAN ION 6.1 No action needed. Prisma SD-WAN ION 5.6 No action needed.

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.