



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Tuesday, August 11, 2026

CAL-CSIC-202608-A-004

Authentication Vulnerability Identified Within Palo Alto Networks GlobalProtect Portal and Gateway

Unauthorized VPN Connection

Conditional Exploit

Limited Exploitation

Update Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high-rated vulnerability found in Palo Alto Networks (PAN) GlobalProtect portal and gateway. CVE-2026-0257 is an authentication bypass vulnerability that carries a CVSS 4.0 score of 7.8.¹

CVE-2026-0257 is an Authentication Bypass vulnerability that impacts PAN GlobalProtect portals and gateways under a certain certificate configuration and when authentication override cookies are enabled. Successful exploitation would enable the attacker to bypass authentication requirements and establish an unauthorized VPN connection.²

Palo Alto Networks has acknowledged the vulnerability and has issued an advisory with mitigation and update guidance that addresses CVE-2026-0257.³ PAN is aware of limited exploitation attempts on unpatched PAN-OS devices without mitigations applied. CVE-2026-0257 was placed in CISA's Known Exploited Vulnerabilities catalog.

The Cal-CSIC recommends following PAN mitigation and update guidance as soon as possible.

For additional details regarding CVE-2026-0257 please use this link:

CVE-2026-0257 Security Advisory: <https://security.paloaltonetworks.com/CVE-2026-0257>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Products and Versions⁴

Product	Affected Version	Unaffected Version
Pan-OS 12.1	< 12.1.4-h6 < 12.1.7	>= 12.1.4-h6 >= 12.1.7
PAN-OS 11.2	< 11.2.4-h17 < 11.2.7-h14 < 11.2.10-h7 < 11.2.12	>= 11.2.4-h17 >= 11.2.7-h14 >= 11.2.10-h7 >= 11.2.12
PAN-OS 11.1	< 11.1.4-h33 < 11.1.6-h32 < 11.1.7-h6 < 11.1.10-h25 < 11.1.13-h5 < 11.1.15	>= 11.1.4-h33 >= 11.1.6-h32 >= 11.1.7-h6 >= 11.1.10-h25 >= 11.1.13-h5 >= 11.1.15
PAN-OS 10.2	< 10.2.7-h34 < 10.2.10-h36 < 10.2.13-h21 < 10.2.16-h7 < 10.2.18-h6	>= 10.2.7-h34 >= 10.2.10-h36 >= 10.2.13-h21 >= 10.2.16-h7 >= 10.2.18-h6
Prisma Access 11.2.0	< 11.2.7-h13	>= 11.2.7-h13
Prisma Access 10.2.0	< 10.2.10-h36	>= 10.2.10-h36

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

References

¹ OpenCVE; "CVE-2026-0257"; <https://app.opencve.io/cve/CVE-2026-0257>; accessed 11 August 2026

² Palo Alto Networks; "CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities"; <https://security.paloaltonetworks.com/CVE-2026-0257>; accessed 11 August 2026

³ Palo Alto Networks; "CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities"; <https://security.paloaltonetworks.com/CVE-2026-0257>; accessed 11 August 2026

⁴ Palo Alto Networks; "CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities"; <https://security.paloaltonetworks.com/CVE-2026-0257>; accessed 11 August 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR