Palo Alto Products Multiple Vulnerabilities

Severity Level: HIGH

Components Affected

- GlobalProtect App 6.0 versions earlier than 6.0.11 on Linux
- GlobalProtect App 6.0 versions earlier than 6.0.13 on macOS and Windows
- GlobalProtect App 6.0 versions earlier than 6.0.14 on Android and ChromeOS
- GlobalProtect App 6.1 versions earlier than 6.1.13 on Android and ChromeOS
- GlobalProtect App 6.2 versions earlier than 6.2.8-h10 (6.2.8-948) on macOS and Windows
- GlobalProtect App 6.3 versions earlier than 6.3.3-h2 (6.3.3-42) on Linux
- GlobalProtect App 6.3 versions earlier than 6.3.3-h9 (6.3.3-999) on macOS and Windows
- PAN-OS 10.2 versions earlier than 10.2.7-h34
- PAN-OS 10.2 versions earlier than 10.2.10-h36
- PAN-OS 10.2 versions earlier than 10.2.13-h21
- PAN-OS 10.2 versions earlier than 10.2.16-h7
- PAN-OS 10.2 versions earlier than 10.2.18-h6
- PAN-OS 11.1 versions earlier than 11.1.4-h33
- PAN-OS 11.1 versions earlier than 11.1.6-h32
- PAN-OS 11.1 versions earlier than 11.1.7-h6
- PAN-OS 11.1 versions earlier than 11.1.10-h25
- PAN-OS 11.1 versions earlier than 11.1.13-h5
- PAN-OS 11.1 versions earlier than 11.1.15
- PAN-OS 11.2 versions earlier than 11.2.4-h17
- PAN-OS 11.2 versions earlier than 11.2.7-h14
- PAN-OS 11.2 versions earlier than 11.2.10-h7
- PAN-OS 11.2 versions earlier than 11.2.12
- PAN-OS 12.1 versions earlier than 12.1.4-h6
- PAN-OS 12.1 versions earlier than 12.1.7
- Prisma Access 10.2.0 versions earlier than 10.2.10-h36
- Prisma Access 11.2.0 versions earlier than 11.2.7-h13

Overview

Multiple security vulnerabilities have been identified in Palo Alto Networks products. These vulnerabilities could allow attackers to gain unauthorized access, execute malicious code, elevate privileges, disrupt services, or bypass implemented security controls. Successful exploitation may affect the confidentiality, integrity, and availability of affected systems.

Description

CVE-2026-0257 is being scattered exploited. Authentication bypass vulnerabilities in the GlobalProtect portal and gateway of PAN-OS software allows the attacker to bypass security restrictions and establish an unauthorized VPN connection.

Impact

- Remote Code Execution
- Denial of Service
- Security Restriction Bypass
- Cross-Site Scripting
- Elevation of Privilege

Solution/ Workarounds

Before installation of the software, please visit the vendor web-site for more details.

Apply fixes issued by the vendor:

- https://security.paloaltonetworks.com/
- https://security.paloaltonetworks.com/CVE-2026-0249
- https://security.paloaltonetworks.com/CVE-2026-0250
- https://security.paloaltonetworks.com/CVE-2026-0251
- https://security.paloaltonetworks.com/CVE-2026-0256
- https://security.paloaltonetworks.com/CVE-2026-0257
- https://security.paloaltonetworks.com/CVE-2026-0258
- https://security.paloaltonetworks.com/CVE-2026-0261
- https://security.paloaltonetworks.com/CVE-2026-0262
- https://security.paloaltonetworks.com/CVE-2026-0263
- https://security.paloaltonetworks.com/CVE-2026-0264
- https://security.paloaltonetworks.com/CVE-2026-0265

Reference

- https://security.paloaltonetworks.com/CVE-2026-0257
- https://www.hkcert.org/security-bulletin/palo-alto-products-multiple-vulnerabilities_20260514

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.