مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability (CVE-2026-0257)

Tracking #:432319039

Date:30-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity authentication bypass vulnerability affecting PAN-OS GlobalProtect portal and gateway components is being actively exploited in the wild. Successful exploitation may allow attackers to bypass authentication controls and establish unauthorized VPN connections on affected devices configured with authentication override cookies under specific certificate conditions.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-0257
- **Severity:** High | **CVSS:** 7.8
- An authentication bypass vulnerability in PAN-OS GlobalProtect portal and gateway components allows attackers to bypass security restrictions and gain unauthorized VPN access. The issue stems from improper validation and integrity protection of authentication override cookies under certain configurations.
- Palo Alto Networks has confirmed that limited exploitation attempts against unpatched devices have been observed.

Affected Products and Versions

- PAN-OS 12.1: Versions earlier than 12.1.4-h6 and 12.1.7
- PAN-OS 11.2: Versions earlier than 11.2.4-h17, 11.2.7-h14, 11.2.10-h7, and 11.2.12
- PAN-OS 11.1: Versions earlier than 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5, and 11.1.15
- PAN-OS 10.2: Versions earlier than 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, and 10.2.18-h6
- Prisma Access 11.2.0: Earlier than 11.2.7-h13
- Prisma Access 10.2.0: Earlier than 10.2.10-h36

Fixed Versions:

PAN-OS 12.1

- Versions 12.1.5 through 12.1.6 → Upgrade to 12.1.7 or later.
- Versions 12.1.2 through 12.1.4-h* → Upgrade to 12.1.4-h6 or 12.1.7 or later.

PAN-OS 11.2

- Version 11.2.11 or later → Upgrade to 11.2.12 or later.
- Versions 11.2.8 through 11.2.10-h* → Upgrade to 11.2.10-h7 or 11.2.12 or later.
- Versions 11.2.5 through 11.2.7-h* → Upgrade to 11.2.7-h14 or 11.2.12 or later.
- Versions 11.2.0 through 11.2.4-h* → Upgrade to 11.2.4-h17 or 11.2.12 or later.

PAN-OS 11.1

- Version 11.1.14 or later → Upgrade to 11.1.15 or later.
- Versions 11.1.11 through 11.1.13-h* → Upgrade to 11.1.13-h5 or 11.1.15 or later.
- Versions 11.1.8 through 11.1.10-h* → Upgrade to 11.1.10-h25 or 11.1.15 or later.
- Versions 11.1.7 through 11.1.7-h* → Upgrade to 11.1.7-h6 or 11.1.15 or later.
- Versions 11.1.5 through 11.1.6-h* → Upgrade to 11.1.6-h32 or 11.1.15 or later.
- Versions 11.1.0 through 11.1.4-h* → Upgrade to 11.1.4-h33 or 11.1.15 or later.

PAN-OS 10.2

- Versions 10.2.17 through 10.2.18-h* → Upgrade to 10.2.18 or 10.2.18-h6 or later.

- Versions 10.2.14 through 10.2.16-h* → Upgrade to 10.2.16-h7 or 10.2.18-h6 or later.
- Versions 10.2.11 through 10.2.13-h* → Upgrade to 10.2.13-h21 or 10.2.18-h6 or later.
- Versions 10.2.8 through 10.2.10-h* → Upgrade to 10.2.10-h36 or 10.2.18-h6 or later.
- Versions 10.2.0 through 10.2.7-h* → Upgrade to 10.2.7-h34 or 10.2.18-h6 or later.

All older unsupported PAN-OS versions → Upgrade to a supported fixed version.

Prisma Access 10.2

- Versions 10.2.0 through 10.2.10-h* → Upgrade to 10.2.10-h36 or later.

Prisma Access 11.2

- Versions 11.2.0 through 11.2.7-h* → Upgrade to 11.2.7-h13 or later.

Mitigations:

- Configure a dedicated certificate exclusively for Authentication Override cookies and avoid certificate reuse.
- Disable Authentication Override by disabling cookie generation and acceptance settings in GlobalProtect portal and gateway configurations.
- Verify whether Authentication Override cookies are enabled on both GlobalProtect portals and gateways and review certificate usage.

Note:

Following upgrades, GlobalProtect users will be required to re-authenticate once because authentication override cookies will be regenerated using a more secure method.

RECOMMENDATIONS:

- Prioritize patching internet-facing GlobalProtect deployments.
- Audit GlobalProtect configurations to identify systems using authentication override cookies.
- Monitor VPN authentication logs for suspicious or unauthorized access attempts.
- Review certificate management practices and isolate authentication override certificates.
- Ensure unsupported PAN-OS versions are migrated to supported releases as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://security.paloaltonetworks.com/CVE-2026-0257