Palo Alto Networks Management Interface Vulnerability

CVE-2024-0012 and CVE-2024-9474

Over 2,000 Palo Alto firewalls exploited in a recent chain exploit.

Overview

Newly discovered vulnerabilities on the **Palo Alto Networks Management Interface** CVE-2024-0012 (CVSS Score: 9.3) and CVE-2024-9474 (CVSS Score: 6.9) have been actively exploited in the wild.

These vulnerabilities are a combination of authentication bypass and privilege escalation that would allow an attacker access to the firewall to perform malicious actions such as modifying configurations and executing arbitrary code with root privileges.

The vulnerabilities are being weaponized to achieve command execution and drop malware, such as *PHP-based web shells* on the hacked firewalls. A functional exploit chaining the two vulnerabilities is publicly available enabling broader threat activity. Additionally, manual and automated scanning has been observed necessitating users to apply latest patches as soon as possible and secure access to the management interface.

Overall Risk

- **Data Breach** – Exfiltration of sensitive information from compromised firewalls
- **Service Disruption** – Firewall tampering could cause network outages or service downtime
- **Reputation Damage** – Loss of Trust due to perceived lack of robust cybersecurity
- **Regulatory Fines** – Due to breach of compliance regulations such as GDPR, HIPPA

Affected Products

Versions	Affected Versions	Unaffected
PAN-OS 11.2	< 11.2.4-h1	>= 11.2.4-h1
PAN-OS 11.1	< 11.1.5-h1	>= 11.1.5-h1
PAN-OS 11.0	< 11.0.6-h1	>= 11.0.6-h1
PAN-OS 10.2	< 10.2.12-h2	>= 10.2.12-h2
PAN-OS 10.1	None	All
Cloud NGFW	None	All
Prisma Access	None	All

Cloud Next Generation Firewall (NGFW) and Prisma Access are not impacted by the vulnerabilities.

Indicators of Compromise (IoCs)

Malicious activity was observed originating from the below IP addresses targeting PAN-OS management web interface Ips accessible over the internet.

- 136.144.17[.]*
- 173.239.218[.]251
- 216.73.162[.]*

The IPs may possibly represent third-party VPNs with legitimate user activity to other destinations.

Additional threat indicators include exploitation patterns and specific techniques used by attackers such as:

- **HTTP Request Headers:** Exploitation of CVE-2024-0012 can involve unauthorized requests with the `X-PAN-AUTHCHECK: off` header, bypassing authentication on the firewall's management interface.
- **Log File Changes:** Accessing or manipulating files such as `/php/uiEnvSetup.php` or `/var/appweb/htdocs/php-packages/panui_core/src/log/Auditlog.php`

Mitigation Strategies

Palo Alto users should patch their systems as soon as possible and ensure their systems are not reachable from the public internet.

Access to the management interface should only be possible from trusted internal IP addresses and not from the internet.

References:

https://security.paloaltonetworks.com/CVE-2024-0012

https://www.bleepingcomputer.com/news/security/over-2-000-palo-alto-firewalls-hacked-using-recently-patched-bugs/