CERT-EU

Security Advisory 2024-117

Zero-Day Vulnerabilities in Palo Alto Networks PAN-OS

2024-11-19 — v1.0

TLP:CLEAR

History:

- *19/11/2024 — v1.0 – Initial publication*

Summary

Palo Alto Networks released security updates for two actively exploited zero-day vulnerabilities in Palo Alto Networks PAN-OS. If exploited, these vulnerabilities could allow a remote unauthenticated attacker to gain administrator privileges, or a PAN-OS administrator to perform actions on the firewall with root privileges [1,2].

It recommended applying the updates and restricting the access to the management web interface to only trusted internal IP addresses, according to the vendor's best practice deployment guidelines [3].

Technical Details

The vulnerability **CVE-2024-0012**, with a CVSS score of 9.3, is an authentication bypass flaw in Palo Alto Networks PAN-OS software. It enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474 [1].

The vulnerability **CVE-2024-9474**, with a CVSS score of 6.9, is a privilege escalation flaw in Palo Alto Networks PAN-OS software. It allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges [2].

Affected Products

The following PAN-OS versions are affected by **CVE-2024-0012** and **CVE-2024-9474**:

- PAN-OS 11.2 before 11.2.4-h1
- PAN-OS 11.1 before 11.1.5-h1
- PAN-OS 11.0 before 11.0.6-h1
- PAN-OS 10.2 before 10.2.12-h2

The PAN-OS 10.1 versions before 10.1.14-h6 are also affected by **CVE-2024-9474**.

Recommendations

CERT-EU recommends applying updates to the affected devices as soon as possible. It is also strongly recommended restricting access to the management web interface.

References

[1] https://security.paloaltonetworks.com/CVE-2024-0012

[2] https://security.paloaltonetworks.com/CVE-2024-9474

[3] https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431