April 12, 2024

Cyber Alert

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Palo Alto Networks published a security advisory about a critical vulnerability (CVE-2024-3400) impacting the GlobalProtect Gateway feature in PAN-OS 11.1, 11.0 and 10.2[Footnote1]. In response to this advisory, the Cyber Centre released advisory AV24-198 on April 12

Technical Details

On April 12, 2024, Palo Alto Networks published a security advisory about a critical vulnerability (CVE-2024-3400) impacting the GlobalProtect Gateway feature in PAN-OS 11.1, 11.0 and 10.2[Footnote1]. In response to this advisory, the Cyber Centre released advisory AV24-198 on April 12[Footnote2].

Exploitation of CVE-2024-3400 may allow an unauthenticated threat actor to execute arbitrary code with root privileges on the firewall[ootnote1]. Palo Alto Networks is aware of limited exploitation of CVE-2024-3400.

This vulnerability affects the following PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls with the configurations for both GlobalProtect gateway and device telemetry enabled:

- PAN-OS 11.1 – versions prior to 11.1.2-h3
- PAN-OS 11.0 – versions prior to 11.0.4-h1
- PAN-OS 10.2 – versions prior to 10.2.9-h1

Fixes for this vulnerability are in development and are expected to be released by April 14[note1].

Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Suggested Action

For affected versions, organizations should determine if they are vulnerable by verifying whether they have a GlobalProtect gateway configured by checking for entries in their firewall web interface (Network > GlobalProtect > Gateways) and verifying whether they have device telemetry enabled by checking their firewall web interface (Device > Setup > Telemetry).

The Cyber Centre strongly recommends that organizations patch affected firewalls when fixes are made available.

Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 95187 (introduced in Applications and Threats content version 8833-8682).

In addition to enabling Threat ID 95187, customers must ensure vulnerability protection has been applied to their GlobalProtect interface to prevent exploitation of this issue on their device[Footnote1].

If you are unable to apply the Threat Prevention based mitigation at this time, you can still mitigate the impact of this vulnerability by temporarily disabling device telemetry until the device is upgraded to a fixed PAN-OS version. Once upgraded, device telemetry should be re-enabled on the device[Footnote1].

The Cyber Centre recommends organizations review open source resources for additional information and indicators of compromise[Footnote3Footnote4].

Organizations should also review and implement the Cyber Centre's Top 10 IT Security Actions[Footnote5] with an emphasis on the following topics:

- Consolidating, monitoring, and defending Internet gateways.
- Patching operating systems and applications.
- Isolate web-facing applications.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-3400,

Information provided by organizations not subject to the *Official Languages Act* is in the language(s) provided.

[1] CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway

[2] AV24-198 – Palo Alto Networks security advisory

[3] Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400

[4]

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)

5