April 17, 2024

Cyber Alert

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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. In response to this advisory, the Cyber Centre released advisory AV24-198 on April 12

Exploitation of CVE-2024-3400 may allow an unauthenticated threat actor to execute arbitrary code with root privileges on the firewall. 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

Technical Details

Update 1

On April 14, 2024, Palo Alto Networks released hotfixes for PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, and PAN-OS 11.1.2-h. Hotfixes for additional versions will be made available in the coming days.

Update 2

On April 17, 2024, Palo Alto Networks updated their security advisory to reflect that having device telemetry disabled does NOT protect PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway and/or GlobalProtect portal from exploitation.

With the GlobalProtect portal product now added as a vulnerable configuration, Palo Alto Networks no longer recommends this as a mitigation and clients with affected versions are advised to apply the hotfixes.

Palo Alto Networks has also provided additional Threat Prevention Threat IDs 95189 and 95191 (available in Applications and Threats content version 8836-8695 and later). Customers with a Threat Prevention subscription can leverage the new signatures for detection and prevention.

Clients can verify whether they have a GlobalProtect gateway or GlobalProtect portal configured by checking for entries in their firewall web interface (Network > GlobalProtect > Gateways or Network > GlobalProtect > Portals).

To reflect the updated guidance from Palo Alto Networks, the Cyber Centre has removed the recommendation to disable telemetry as a mitigation strategy.

Action Required

Update April 17 2024

Clients can verify whether they have a GlobalProtect gateway or GlobalProtect portal configured by checking for entries in their firewall web interface (Network > GlobalProtect > Gateways or Network > GlobalProtect > Portals).

To reflect the updated guidance from Palo Alto Networks, the Cyber Centre has removed the recommendation to disable telemetry as a mitigation strategy.

Partner Reporting

- ACSC - OS Command Injection Vulnerability in GlobalProtect Gateway
- NCSC-NZ - Palo Alto Command Injection Vulnerability in PAN-OS GlobalProtect

References

- CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway
- AV24-198 – Palo Alto Networks security advisory
- Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400
- Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- Palo Alto Networks product downloads (Login required)