SamCERT Advisory

22nd April 2024

Palo Alto Command Injection Vulnerability in PAN-OS GlobalProtect

A critical vulnerability (CVE-2024-3400) is being exploited and may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

This vulnerability affects certain Palo Alto Networks Operating System (PAN-OS) products using GlobalProtect Gateway.

Patches are now available, and we encourage organisations to continue monitoring the vendor advisory for further updates. Note that mitigation actions have been changed (17/04/2024).

What is happening and systems affected.

This vulnerability applies to the following versions of PAN-OS and requires configurations for both GlobalProtect gateway and device telemetry to be enabled.

- PAN-OS 11.1 – versions earlier than 11.1.2-h3
- PAN-OS 11.0 – versions earlier than 11.0.4-h1
- PAN-OS 10.2 – versions earlier than 10.2.9-h1

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

What to look for and how to tell if you're at risk.

You can upload a Technical Support File (TSF) to the Palo Alto Customer Support Portal (CSP) to determine if your device logs match known indicators of compromise (IoC).

What to do to prevent it.

Patches are available for this vulnerability.
Upgrade your Palo Alto PAN-OS to one of the following versions (or later).

- 11.1.2-h3
- 11.0.4-h1
- 10.2.9-h1

Check the Palo Alto Networks site for updates on this. (CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect (paloaltonetworks.com)

Hotfixes for other commonly deployed maintenance releases will also be made available to address this issue.

Mitigation

Threat Prevention subscribers can block attacks for this vulnerability by enabling Threat ID 95187.

NOTE: Our original advisory said to disable device telemetry as a mitigation; the vendor advises this is no longer the case.