April 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Palo Alto Networks published a security advisory to address a vulnerability in the following products:

- PAN-OS 11.1 – versions prior to 11.1.2-h3
- PAN-OS 11.0 – versions prior to 0.4-h1
- PAN-OS 10.2 – versions prior to 10.2.9-h1

Exploitation of this vulnerability could lead to remote code execution. Palo Alto Networks has indicated that CVE-2024-3400 has been exploited.

Technical Details

A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Fixes for PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 are in development and are expected to be released by April 14, 2024. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. All other versions of PAN-OS are also not impacted.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2024-3400 CVE-2024-3383 CVE-2024-3385 CVE-2024-3382 CVE-2024-3384 CVE-2024-3386 CVE-2024-3387 CVE-2024-3388
- Palo Alto Networks Security Advisory - CVE-2024-3400
- Palo Alto Network Security Advisories