SECURITY ADVISORY

CRITICAL SEVERITY COMMAND INJECTION VULNERABILITY IN PALO ALTO NETWORKS GLOBAL PROTECT (CVE-2024-3400)

Lodestone Security

UPDATED ON: APRIL 17TH, 2024

Table of Contents

Executive Summary

On April 12, 2024, Palo Alto Networks disclosed a critical command injection vulnerability identified as CVE-2024-3400, impacting certain configurations of its PAN-OS software. This vulnerability allows unauthenticated attackers to execute arbitrary commands with root privileges. It affects only devices running PAN-OS 10.2, 11.0, and 11.1 with **both** GlobalProtect gateway **and** device telemetry features enabled. Security patches were released on April 14th, and Palo Alto has provided temporary mitigations through "Threat Prevention Signatures".

For details on how to implement the workarounds, please review the "Mitigations / Workarounds" section of this advisory.

Update (2024-04-17 14:00 UTC) – Palo Alto Networks has discovered that the previously recommended mitigation of disabling device telemetry is **ineffective** in preventing successful exploitation of this vulnerability. Maintaining an active "Threat Prevention" subscription and enabling signatures for **Threat IDs 95187, 95189** and **95191** on the GlobalProtect interface, however, continues to offer some protection.

Lodestone Labs has observed an increase in mass scanning activities targeting potentially vulnerable Palo Alto devices and widespread attempts to exploit this vulnerability. Given the role of Palo Alto's GlobalProtect as an internet-facing remote access VPN solution, and given the vulnerability's ease of exploitation, Lodestone Labs strongly recommends that organizations apply Palo Alto's latest patches **immediately** rather than rely on mitigations.

Update (2024-04-16 07:30 UTC) – A public proof-of-concept (PoC) exploit has been disclosed by security researchers on twitter. The vulnerability in Palo Alto GlobalProtect devices is trivial to exploit. Lodestone Labs expects to see mass scanning and exploit attempts across internet exposed devices in the coming few hours. Palo Alto Networks has now released patches for this vulnerability for the following PAN-OS releases:

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

Palo Alto has also published expected release dates for their maintenance releases on their website.

Given the ease of exploitability for this vulnerability and the release of a public PoC, Lodestone strongly recommends that organizations take **immediate action** to patch these vulnerabilities or to apply the workarounds / mitigations described below.

Update (2024-04-13 01:30 UTC) – CVE-2024-3400 is under active exploitation by a highly competent, well-sourced nation-state threat actor using a weaponized exploit. Security firm Volexity, who made the

initial discovery of this vulnerability, reported seeing attack attempts as early as 2024-03-26. A publicly available version of this exploit is not known to exist at the time of this update. However, we expect cybercriminal threat actors to develop and deploy exploits in the coming days and weeks.

Affected Systems / Products

The vulnerability affects the following PAN-OS versions if the GlobalProtect (VPN) feature AND device telemetry collection are enabled:

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

Mitigations / Workarounds

Palo Alto Networks has provided two workarounds for organizations leveraging GlobalProtect with device telemetry collection enabled.

Organizations with an active "Threat Prevention" subscription

Update (2024-04-17 14:00 UTC) – Palo Alto has added **Threat IDs 95189** and **95191** to detect attacks against this vulnerability.

Organizations with an active "Threat Prevention" subscription should enable the signatures for **Threat IDs 95187, 95189, and 95191**. Additionally, organizations must ensure that vulnerability protection is enabled on the GlobalProtect interface in order for this mitigation to be effective.

Organizations without an active Threat Prevention subscription

Update (2024-04-17 14:00 UTC) – Palo Alto has warned that this mitigation for organizations without an active Threat Prevention subscription **is no longer effective** and should not be applied. Organizations should instead apply available patches immediately.

~~Organizations without an active Threat Prevention subscription or those who are unable to apply the signature described above should disable device telemetry collection (which is enabled by default) by following the instructions below:~~

1. Log in to the Palo Alto administrative web interface as an administrator.
2. Navigate to the "Device" tab.
3. Click on "Telemetry" settings.
4. Find the "Device Telemetry" section.
5. Uncheck the box or select the “disable” option for "Enable Device Telemetry."
6. Save your changes to apply the new settings.

Patches

Hotfix releases for affected PAN-OS versions **were released April 14, 2024**. Lodestone Labs recommends that organizations apply applicable patches as soon as possible as this vulnerability is under active widespread exploitation.

How Lodestone is Responding

Lodestone is monitoring client perimeter devices discovered by Karma for partners to assist organizations in remediating any issues found.

Sources

- https://security.paloaltonetworks.com/CVE-2024-3400
- https://unit42.paloaltonetworks.com/cve-2024-3400/
- https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
- https://twitter.com/HackingLZ/status/1780239802496864474