Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Report

Critical OS Command Injection in GlobalProtect Gateway

NSAI

QUALITY
I.S. EN ISO 27001:2013
NSAI Certified

QUALITY
I.S. EN ISO 9001:2015
NSAI Certified

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	02
Authors	Marian Matache <marian.matache@smarttech247.com>
Verified by	Alin Curcan <alin.curcan@smarttech247.com>
Last modified	2024-04-12
Issue Date	2024-04-12

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.

Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

A critical vulnerability, CVE-2024-3400, has been identified in Palo Alto Networks PAN-OS software, specifically affecting versions 10.2, 11.0, and 11.1 with specific GlobalProtect gateway and device telemetry configurations. This flaw could allow an unauthenticated attacker to execute arbitrary code with root privileges on affected firewalls.

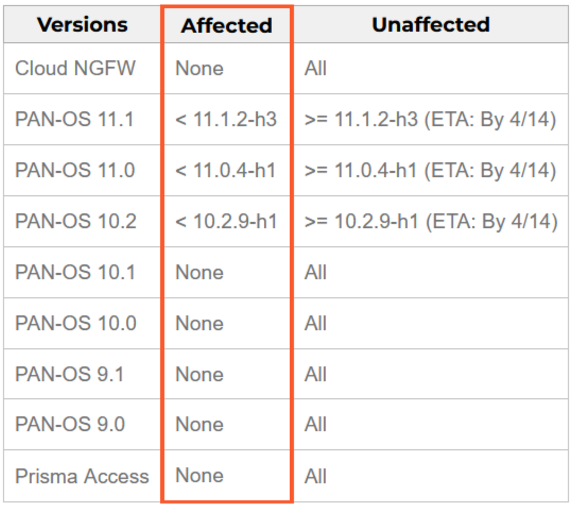
TECHNICAL SUMMARY

CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway.

CVSSv4.0 Base Score: 10

CVE-2024-3400 is a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software and may allow an unauthenticated attacker to execute arbitrary code with root privileges on vulnerable firewalls.

Affected Products



Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.2-h3	>= 11.1.2-h3 (ETA: By 4/14)
PAN-OS 11.0	< 11.0.4-h1	>= 11.0.4-h1 (ETA: By 4/14)
PAN-OS 10.2	< 10.2.9-h1	>= 10.2.9-h1 (ETA: By 4/14)
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

Exploitation Status

Palo Alto Networks is aware of a limited number of attacks that leverage the exploitation of this vulnerability.

Solution

- **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.
- Verify whether you have a GlobalProtect gateway configured by checking for entries in your firewall web interface (Network > GlobalProtect > Gateways) and verify whether you have device telemetry enabled by checking your firewall web interface (Device > Setup > Telemetry).
- "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)."
- Apply a vulnerability protection security profile to the GlobalProtect interface to prevent exploitation of this issue on their device.
- Mitigate the impact of this vulnerability by temporarily disabling device telemetry (and then re-enable it once the hotfix is applied).

References

Palo Alto:

https://security.paloaltonetworks.com/CVE-2024-3400
https://www.helpnetsecurity.com/2024/04/12/cve-2024-3400/

CVE:

CVE-2024-3400