NEWSFLASH

Don't Get Hacked: Fixing the PAN-OS Flaw

NANGIA & CO LLP

What is the vulnerability

A zero-day 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. Tracked as **CVE-2024-3400**, the issue has a CVSS score of 10.0, indicating maximum severity.

Threat actors have been able to exploit the vulnerability to compromise the firewall to introduce a python based backdoor, create a reverse shell, download further tools on the device, exfiltrate data and move laterally within the network. The exact origins of the threat actor exploiting the flaw are presently unknown but Palo Alto Networks Unit 42 is tracking the malicious activity under the name **Operation MidnightEclipse**.

What is affected?

The flaw impacts the following versions of PAN-OS

PAN-OS < 11.1.2-h3

PAN-OS < 11.0.4-h1

PAN-OS < 10.2.7-h8, < 10.2.8-h3 , < 10.2.9-h1

The company also said that the issue applies only to firewalls that have the configurations for both GlobalProtect gateway (Network > GlobalProtect > Gateways) and device telemetry (Device > Setup > Telemetry) enabled.

How do you protect yourself?

This issue is fixed in hotfix releases of PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, PAN-OS 11.1.2-h3, and in all later PAN-OS versions. Hotfixes for other commonly deployed maintenance releases will also be made available to address this issue. Palo Alto Networks states that hotfixes for rest of the versions will be released by the date 19/04/2024.

NANGIA & CO LLP

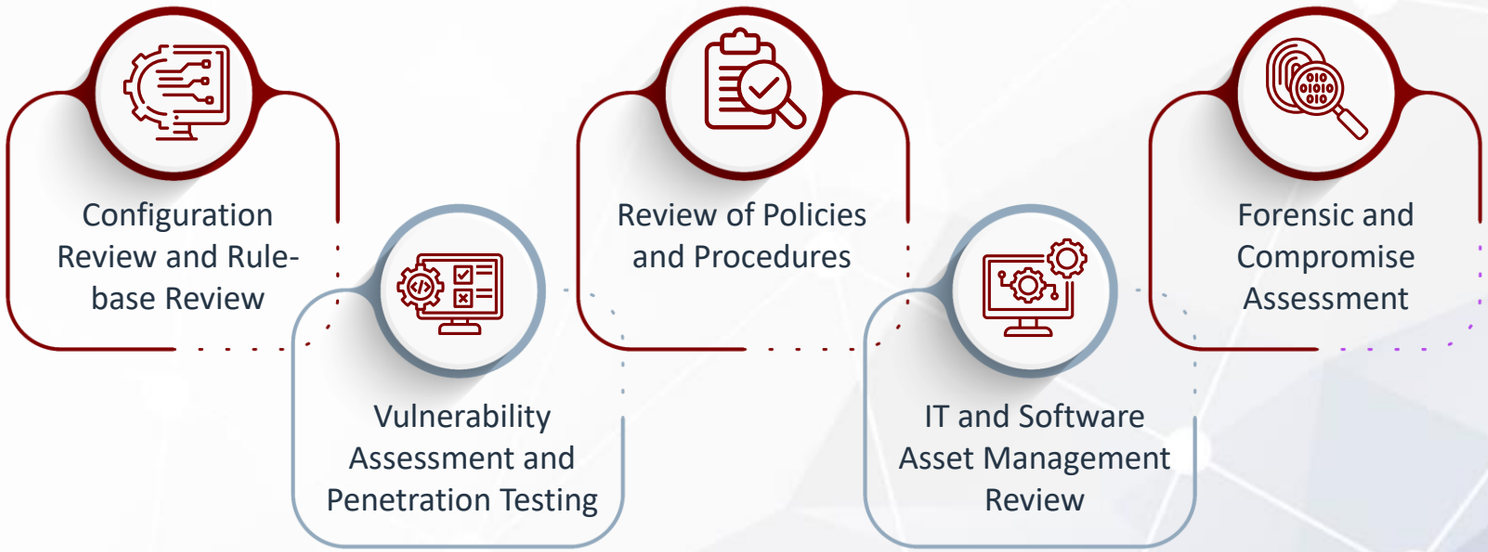
Mitigations and Workarounds

Customers with a Threat Prevention subscription of Palo Alto can block attacks for this vulnerability using Threat ID 95187 (available in Applications and Threats content version 8833-8682 and later). To apply Threat ID 95187, it must be ensured that vulnerability protection has been applied to the GlobalProtect interface to prevent exploitation of this issue on the device.

If you are unable to apply the Threat Prevention based mitigation at this time, you can still mitigate the impact of this vulnerability by temporarily disabling device telemetry until the device is upgraded to a fixed PAN-OS version. Once upgraded, device telemetry should be re-enabled on the device. If the firewalls are managed by Panorama, ensure that device telemetry is disabled in relevant templates (Panorama > Templates).

Additionally, it is recommended to conduct regular penetration testing, vulnerability assessments, configuration audits and rule-base reviews to fortify network defenses.

How can Nangia & Co LLP help?



NANGIA & CO LLP

NOIDA
(Delhi NCR - Corporate Office) A-109, Sector - 136, Noida - 201304, India
T: +91 120 2598000

DELHI
(Registered Office) B-27, Soami Nagar, New Delhi - 110017, India T: +91 120 2598000

GURUGRAM
001-005, Emaar Digital Greens Tower-A 10th Floor, Golf Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

MUMBAI
4th Floor, Iconic Tower, URMI Estate, Ganpat Rao Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

CHENNAI
Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand Lights, Chennai - 600006 T: +91 44 46549201

BENGALURU
Prestige Obelisk, Level 4, No 3 Kasturba Road, Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

PUNE
3rd Floor, Park Plaza, CTS 1085, Ganeshkhind Road, Next to Pune Central Mall, Shivajinagar, Pune - 411005, India

DEHRADUN
1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001, Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

Follow us at:

NANGIA & CO LLP