HC3: Sector Alert

April 18, 2024 TLP:CLEAR Report: 202404181500

Update: Palo Alto Networks Firewalls (CVE-2024-3400)

Executive Summary

On April 12, 2024, Palo Alto Networks issued a warning about CVE-2024-3400, a zero-day command injection vulnerability found in its firewalls operating PAN-OS v10.2, 11.0, and 11.1 with configurations for both GlobalProtect gateway and device telemetry enabled. There have been an increasing number of attacks observed against this vulnerability since its release. In the original advisory, it was believed that disabling device telemetry would work as an effective secondary mitigation, but the most recent update states that device telemetry does not need to be enabled for PAN-OS to be vulnerable to attacks. Hotfixes were also released starting on April 14, 2024. HC3 strongly encourages all organizations to review the updated security advisory and apply any mitigations to prevent serious damage from occurring to the Healthcare and Public Health (HPH) sector.

Report

Palo Alto's updated security advisory, released on April 17, 2024, noted that they were aware of an increasing number of attacks targeting CVE-2024-3400, and the proof of concept was publicly disclosed. Reports from Unit 42 show that threat actors are using this vulnerability to set up a backdoor and leverage the access gained to move through target organizations' networks Additionally, reports from ShadowServer show that approximately 156,000 instances have been seen daily. Palo Alto is monitoring this vulnerability under the name Operation MidnightEclipse. For further information regarding the details of this attack, including indicators of compromise, please refer to this link. Additional information on the vulnerability from Volexity can be found here. For the most up-to-date security information, we recommend reviewing Palo Alto's Security Advisory.

Current advisories from Palo Alto Networks report that this vulnerability only affects PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both). Importantly, this issue does not impact cloud firewalls (Cloud NGFW), Panorama appliances, or Prisma Access.

Patches, Mitigations, and Workarounds

According to Palo Alto: “We strongly advise customers to immediately upgrade to a fixed version of PAN-OS to protect their devices even when workarounds and mitigations have been applied. This issue is fixed in 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. Customers who upgrade to these versions will be fully protected. In addition, to provide the most seamless upgrade path for customers, additional hotfixes are being made available as a courtesy for other commonly deployed maintenance releases and will also be made available to address this issue. Customers do not have to wait for these hotfixes.”

PAN-OS 10.2:
- 10.2.9-h1 (Released 4/14/24)
- 10.2.8-h3 (Released 4/15/24)
- 10.2.7-h8 (Released 4/15/24)
- 10.2.6-h3 (Released 4/16/24)
- 10.2.5-h6 (Released 4/16/24)

- 10.2.3-h13 (ETA: 4/18/24)
- 10.2.1-h2 (ETA: 4/18/24)
- 10.2.2-h5 (ETA: 4/18/24)
- 10.2.0-h3 (ETA: 4/18/24)
- 10.2.4-h16 (ETA: 4/19/24)

PAN-OS 11.0:
- 11.0.4-h1 (Released 4/14/24)
- 11.0.4-h2 (Released 4/17/24)
- 11.0.3-h10 (Released 4/16/24)
- 11.0.2-h4 (Released 4/16/24)
- 11.0.1-h4 (ETA: 4/18/24)
- 11.0.0-h3 (ETA: 4/18/24)

PAN-OS 11.1:
- 11.1.2-h3 (Released 4/14/24)
- 11.1.1-h1 (Released 4/16/24)
- 11.1.0-h3 (Released 4/16/24)

The manufacturer also announced the following updated mitigations:

- Customers with a Threat Prevention subscription can prevent attacks related to this vulnerability using Threat IDs 95187, 95189, and 95191. These are available in Applications and Threats content version 8836-8695 and beyond.

- To utilize the Threat IDs, customers should make sure vulnerability protection is enabled on their GlobalProtect interface to guard against potential exploitation of this issue on their device. For more details, visit this link.

- Additionally, this updated reflects that disabling device telemetry is no longer considered an effective mitigation.

Users should also monitor their logs thoroughly, even after applying the patch to ensure no prior exploitation has taken place.

Related HC3 Reporting

palo-alto-networks-firewalls-sector-alert-tlpclear.pdf (hhs.gov)

References

Unit 42. Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400. April 12, 2024. https://unit42.paloaltonetworks.com/cve-2024-3400/

Volexity Threat Research. Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400). April 12, 2024. https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Gatlan, Sergiu. Exploit released for Palo Alto PAN-OS bug used in attacks, patch now. Bleeping Computer. April 16, 2024. https://www.bleepingcomputer.com/news/security/exploit-released-for-palo-alto-pan-os-bug-used-in-attacks-patch-now/

Palo Alto. CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway. April 17, 2024. https://security.paloaltonetworks.com/CVE-2024-3400

Zorz, Zeljka. Palo Alto Networks firewalls under attack, hotfixes incoming! (CVE-2024-3400). April 12, 2024. https://www.helpnetsecurity.com/2024/04/12/cve-2024-3400/

Zorz, Zeljka. Palo Alto firewalls: Public exploits, rising attacks, ineffective mitigation. April 17, 2024. https://www.helpnetsecurity.com/2024/04/17/cve-2024-3400-attacks/

Palo Alto. Applying Vulnerability Protection to GlobalProtect Interfaces. Maurisy. April 12, 2024. https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184

NIST. CVE-2024-3400. https://nvd.nist.gov/vuln/detail/CVE-2024-3400

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback