Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

April 12, 2024 TLP: CLEAR Report: 202404121500

Palo Alto Networks Firewalls (CVE-2024-3400)

Executive Summary

On April 12, 2024, Palo Alto Networks has warned of a command injection vulnerability (CVE-2024-3400) impacting its firewalls. The vulnerability can be exploited in an automated manner, and the company recommends that customers apply temporary mitigations. Palo Alto Networks is aware of a limited number of attacks utilizing this vulnerability. HC3 recommends that all users review the security alert released by Palo Alto and apply any mitigations or workarounds to prevent serious damage in the Healthcare and Public Health (HPH) sector.

Report

Palo Alto released a security advisory for CVE-2024-3400, a command injection flaw in the GlobalProtect feature of Palo Alto Networks PAN-OS software that affects certain PAN-OS versions and specific feature configurations. This vulnerability may allow an unauthenticated attacker to run arbitrary code with root privileges on the firewall. The flaw currently impacts the following versions of PAN-OS:

- PAN-OS < 11.1.2-h3
- PAN-OS < 11.0.4-h1
- PAN-OS < 10.2.9-h1

This vulnerability does not impact Cloud NFW, Panorama appliances, or Prisma Access, nor does it affect any other versions of PAN-OS. Researchers have viewed this vulnerability as being exploited in a limited number of attacks. Palo Alto has reported that hotfixes will be released on April 14, 2024, to remediate this issue.

Patches, Mitigations, and Workarounds

The manufacturer advises the following mitigation strategies:

- Customers with a Threat Prevention subscription can protect against this vulnerability by activating Threat ID 95187.
- Along with activating Threat ID 95187, customers should ensure that vulnerability protection is applied to their GlobalProtect interface. More details can be found at this link.
- If implementing Threat Prevention mitigation is not feasible, the vulnerability risk can be reduced by temporarily disabling device telemetry until the device is updated. After upgrading, device telemetry should be re-enabled.
    - Navigate to Device > Setup > Telemetry
    - Edit the Telemetry widget.
    - Uncheck the Enable Telemetry box.
    - Click OK, and then commit your changes.

References

Palo Alto. CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway. April 12, 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/

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