Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

THREAT BULLETINS

Update: Palo Alto Networks Has Released Security Updates to Address Critical Vulnerability CVE-2024-3400

○○○ TLP:WHITE

Apr 15, 2024

Summary:

On April 14, Palo Alto Networks released security updates for the critical unauthenticated remote code execution flaw CVE-2024-3400 affecting GlobalProtect. In the latest update by Volexity, the cyber company who initially discovered the exploitation, the incident is attributed to a threat actor tracked as UTA0218, with the earliest exploitation identified dating back to March 26, 2024.

Analysis:

Palo Alto Networks has released anticipated patches for critical vulnerability CVE-2024-3400, which has a CVSS score of 10/10. CVE-2024-3400 is a critical vulnerability affecting Palo Alto Networks PAN-OS GlobalProtect. The flaw allows unauthenticated attackers to execute code remotely on compromised devices. The flaw was discovered during active exploitation as a zero-day and was reported last Friday, April 12. The exploitation was dubbed Operation Midnight Eclipse. The attackers have leveraged the flaw to pivot and eventually move laterally inside compromised networks to steal sensitive data.

According to a report published by Volexity, the cyber company credited with discovering the exploitation, the threat actor, tracked as UTA0218, exploited firewall devices, created reverse shells, and downloaded tools for further access. A custom Python-based backdoor called UPSTYLE was deployed to execute commands via specially crafted network requests. The earliest identified exploitation attempts date back to March 26, 2024, with successful exploitation and lateral movement observed on April 10 and 11, 2024. The attacker targeted sensitive data, including keys, Active Directory credentials, and user data.

Due to the sophisticated TTPs used, it is suspected that UTA0218 is a state-backed threat actor; however, confident attribution to any state has not yet been made.

More information on the vulnerability can be found in a linked Threat Bulletin previously distributed by Health-ISAC here.

Palo Alto recommends immediately applying available patches. In cases where patching is not available, certain workarounds can be applied; however, these should be considered only temporary solutions until patching is possible.

Recommendations:

- Apply available patches.

- In cases where patching is not available at the moment, possible workarounds are as follows:

1. Palo Alto Threat Prevention subscribers have the option to enable Threat ID 95187 to secure against the threat.
2. Check if a GlobalProtect gateway is configured correctly by going to Network > GlobalProtect > Gateways in the firewall's web interface.
3. Apply vulnerability protection on the GlobalProtect interface.
4. Verify if device telemetry is enabled by going to Device > Setup > Telemetry.
5. Disable device telemetry until fixes are applied.

Reference(s)	Palo Alto Networks, TOC Spotlight Webinar - Citrix Slides Attachment, The Hacker News, Volexity Blog

Sources
Sources:

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)
CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect
Palo Alto Networks Releases Urgent Fixes for Exploited PAN-OS Vulnerability

Alert ID b5b6d0ae

View Alert

Tags CVE-2024-3400, Patches, Palo Alto PAN-OS, Zero-Day

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.