[CS-SU-24-0401] CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway

Palo Alto Networks is facing a serious security threat. A critical vulnerability (CVE-2024-3400) has been discovered in their PAN-OS firewall software that could allow attackers to seize complete control of your firewall. This vulnerability specifically targets PAN-OS versions 10.2, 11.0, and 11.1, but only if two specific features are enabled: GlobalProtect gateway and device telemetry. While attackers are already exploiting this vulnerability, Palo Alto Networks is aware of the issue and expects to release a permanent fix by April 14, 2024.

In the meantime, there are steps you can take to mitigate the risk. If you have a Threat Prevention subscription, enabling Threat ID 95187 can help block these attacks. Another option is to temporarily disable device telemetry. However, it's important to remember that device telemetry is a valuable feature, so you'll want to re-enable it once you've applied the permanent fix from Palo Alto Networks to ensure your firewall has full functionality.

As Palo Alto continues to provide updates and reports on new vulnerabilities, it is critical to implement best security practices, ensure systems and software are up-to-date, and prioritize continuous management of digital infrastructure as cybercriminals continue to exploit known flaws in systems and software.

The CRITICALSTART® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICALSTART® Intelligence Hub.