Palo Alto Networks ha emitido actualizaciones de seguridad para resolver una vulnerabilidad de máxima gravedad que afecta al software PAN-OS y que ha sido objeto de explotación activa en el mundo real.

Identificada como CVE-2024-3400 (puntuación CVSS: 10.0), la vulnerabilidad crítica consiste en una inyección de comandos en la función GlobalProtect, que un atacante no autenticado podría utilizar para ejecutar código arbitrario con privilegios de root en el firewall.

Las soluciones para esta deficiencia están disponibles en las siguientes versiones:

- PAN-OS 10.2.9-h1
- PAN-OS 11.0.4-h1, y
- PAN-OS 11.1.2-h3

Se espera que pronto se lancen parches para otras versiones de mantenimiento comúnmente implementadas.

> *«Este problema solo afecta a los firewalls PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 configurados con el portal de GlobalProtect o la puerta de enlace de GlobalProtect (o ambos) y con telemetría de dispositivo habilitada»,* explicó la compañía en su aviso actualizado.

También se señaló que, aunque los firewalls Cloud NGFW no se ven afectados por CVE-2024-3400, ciertas versiones específicas de PAN-OS y configuraciones de características particulares de los firewalls VM desplegados y gestionados por los clientes en la nube están siendo afectadas.

Los detalles exactos sobre el origen del actor de amenazas que está explotando la vulnerabilidad son desconocidos en este momento, pero Palo Alto Networks Unit 42 está monitoreando la actividad maliciosa bajo el nombre de Operación MidnightEclipse.

Volexity, que atribuyó estos ataques a un grupo llamado UTA0218, informó que CVE-2024-3400 ha sido utilizado desde al menos el 26 de marzo de 2024 para distribuir un backdoor basado en Python llamado UPSTYLE en el firewall, lo cual permite la ejecución de comandos arbitrarios a través de solicitudes especialmente elaboradas.

Aunque no está claro cuán extendida ha sido la explotación, la firma de inteligencia de amenazas indicó tener *«evidencia de actividad de reconocimiento potencial que implica una explotación más amplia dirigida a identificar sistemas vulnerables».*

En los ataques documentados hasta ahora, UTA0218 ha sido visto desplegando cargas útiles adicionales para lanzar shells inversos, extraer datos de configuración de PAN-OS, eliminar archivos de registro y desplegar una herramienta de túnel Golang llamada GOST (GO Simple Tunnel).

Hasta el momento, no se han encontrado otros malware de seguimiento o métodos de persistencia en las redes de las víctimas, aunque se desconoce si esto se debe a un diseño deliberado o a una respuesta temprana de detección.