Palo Alto Networks ha compartido pautas de remedio para una vulnerabilidad crítica de seguridad recientemente divulgada que afecta a PAN-OS y que ha sido objeto de explotación activa.

La vulnerabilidad, identificada como CVE-2024-3400 (puntuación CVSS: 10.0), podría ser aprovechada para obtener ejecución remota de comandos de shell sin autenticación en dispositivos susceptibles. Se ha abordado en múltiples versiones de PAN-OS 10.2.x, 11.0.x y 11.1.x.

Existen indicios que sugieren que el problema ha sido explotado como un día cero desde al menos el 26 de marzo de 2024, por un grupo de amenazas conocido como UTA0218.

La actividad, llamada Operación MidnightEclipse, implica el uso de la vulnerabilidad para insertar una puerta trasera basada en Python llamada UPSTYLE que puede ejecutar comandos transmitidos mediante solicitudes especialmente diseñadas.

Aunque las intrusiones no han sido atribuidas a un actor o grupo de amenazas específico, se sospecha que podría tratarse de un equipo de piratas informáticos respaldado por un estado debido a las técnicas y objetivos observados.

Las últimas recomendaciones de remedio ofrecidas por Palo Alto Networks se basan en el grado de compromiso:

- Nivel 0 de Sondeo: Intento de explotación sin éxito: aplique la última corrección proporcionada.
- Nivel 1 de Prueba: Evidencia de que se está probando la vulnerabilidad en el dispositivo, como la creación de un archivo vacío en el firewall pero sin ejecución de comandos no autorizados: aplique la última corrección proporcionada.
- Nivel 2 de Posible Exfiltración: Señales de que se han copiado archivos como «running_config.xml» a una ubicación accesible a través de solicitudes web: aplique la última corrección proporcionada y realice un Reinicio de Datos Privados.
- Nivel 3 de Acceso Interactivo: Evidencia de ejecución de comandos interactivos, como

la introducción de puertas traseras y otro código malicioso: aplique la última corrección proporcionada y realice un Restablecimiento de Fábrica.

> Palo Alto Networks señaló que *«realizar un restablecimiento de datos privados elimina los riesgos de un posible mal uso de los datos del dispositivo. Se recomienda un restablecimiento de fábrica debido a la evidencia de una actividad de actor de amenazas más agresiva».*