Vulnerabilidad Crítica en PAN-OS de Palo Alto

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Palo Alto ha publicado un aviso de seguridad para tratar **1 vulnerabilidad de severidad crítica**, cuyo identificador es CVE-2024-3400, que afecta al producto **PAN-OS**, el sistema operativo desarrollado por Palo Alto Networks que se utiliza en sus dispositivos de seguridad.

Esta vulnerabilidad supone una amenaza de alta gravedad para la **confidencialidad, integridad** y **disponibilidad** de los sistemas que se puedan ver afectados.

Además, desde Palo Alto Networks se afirma tener **conocimiento de un número limitado de ataques que aprovechan la explotación** de esta vulnerabilidad.

El fabricante ha indicado que la actualización para corregir el fallo está en desarrollo y se espera para el 14 de abril de 2024. Mientras tanto, ofrece medidas de mitigación para mitigar el error hasta que se pueda aplicar el parche correspondiente.

2. Recursos afectados

Los recursos afectados por la vulnerabilidad CVE-2024-3400 son:

- PAN-OS 11.1 en versiones anteriores a la versión 11.1.2-h3.
- PAN-OS 11.0 en versiones anteriores a la versión 11.0.4-h1.
- PAN-OS 10.2 en versiones anteriores a la versión 10.2.9-h1.

3. Análisis técnico

Los detalles de la vulnerabilidad crítica tratada en este aviso son los siguientes:

CVE-2024-3400: vulnerabilidad de inyección de comandos en la función GlobalProtect del software PAN-OS para versiones específicas de PAN-OS y configuraciones de características distintas, que puede permitir a un atacante no autenticado ejecutar código arbitrario con privilegios de root en el firewal. Esta vulnerabilidad no afecta a Cloud NGFW, los dispositivos Panorama y Prisma Access. Tampoco se ven afectadas todas las demás versiones de PAN-OS.

Las versiones de **PAN-OS** afectadas son las siguientes:

- PAN-OS 11.1 en versiones anteriores a la versión 11.1.2-h3.
- PAN-OS 11.0 en versiones anteriores a la versión 11.0.4-h1.
- PAN-OS 10.2 en versiones anteriores a la versión 10.2.9-h1.

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-77: Improper Neutralization of Special Elements used in a Command (Command Injection)

CVSS Base: **10.0**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para corregir la vulnerabilidad CVE-2024-3400, que afecta a las versiones 10.2, 11.0 y 11.1 de PAN-OS, desde Palo Alto se ha indicado que se están desarrollando las correcciones necesarias y se espera que sean publicadas el día 14 de abril de 2024.

Los clientes con una suscripción de Prevención de Amenazas pueden bloquear ataques para esta vulnerabilidad habilitando la Amenaza ID 95187, introducida en la versión de contenido de Aplicaciones y Amenazas 8833-8682.

Además de habilitar la Amenaza ID 95187, los clientes deben asegurarse de que la protección de vulnerabilidades se haya aplicado a su interfaz GlobalProtect para evitar la explotación de este problema en su dispositivo. Más información en el siguiente enlace.

Si no se puede aplicar la mitigación basada en Prevención de Amenazas, se puede mitigar el impacto de esta vulnerabilidad deshabilitando temporalmente la telemetría del dispositivo hasta que se actualice a una versión de PAN-OS corregida. Una vez actualizado, la telemetría del dispositivo debería volver a habilitarse en el dispositivo. Para realizar esta operación se puede consultar el siguiente enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-3400.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY