Vulnerabilidades en PAN-OS de Palo Alto

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

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 avisos de seguridad para tratar **4 vulnerabilidades de severidad alta**, cuyos identificadores son CVE-2024-3383, CVE-2024-3385, CVE-2024-3382 y CVE-2024-3384, las cuales afectan al producto **PAN-OS**, el sistema operativo desarrollado por Palo Alto Networks que se utiliza en sus dispositivos de seguridad.

Las mayorías de estas vulnerabilidades suponen una amenaza de alta gravedad para la integridad y disponibilidad de los sistemas que se puedan ver afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

Los recursos afectados por la vulnerabilidad CVE-2024-3385 son:

- PAN-OS 11.0 en versiones anteriores a la versión 11.0.3.
- PAN-OS 10.2 en versiones anteriores a la versión 10.2.8.
- PAN-OS 10.1 en versiones anteriores a la versión 10.1.12.
- PAN-OS 9.1 en versiones anteriores a la versión 9.1.17.
- PAN-OS 9.0 en versiones anteriores a la versión 9.0.17-h4.

Los recursos afectados por la vulnerabilidad vulnerabilidad CVE-2024-3384 son:

- PAN-OS 10.0 versiones anteriores a la versión 10.0.12.
- PAN-OS 9.1 versiones anteriores a la versión 9.1.15-h1.
- PAN-OS 9.0 versiones anteriores a la versión 9.0.17.
- PAN-OS versiones anteriores a la versión 8.1.24.

Los recursos afectados por la vulnerabilidad vulnerabilidad CVE-2024-3382 son:

- PAN-OS 11.1 versiones anteriores a la 11.1.2.
- PAN-OS 11.0 versiones anteriores a la versión 11.0.4.
- PAN-OS 10.2 versiones anteriores a la versión 10.2.7-h3

Los recursos afectados por la vulnerabilidad CVE-2024-3383 son:

- PAN-OS 11.0 en versiones anteriores a la versión 11.0.3.
- PAN-OS 10.2 en versiones anteriores a la version 10.2.5.
- PAN-OS 10.1 en versiones anteriores a la version 10.1.11.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2024-3385: vulnerabilidad originada debido a un fallo en el mecanismo de procesamiento de paquetes del software PAN-OS que permite a un atacante remoto reiniciar los firewalls basados en hardware. Los ataques repetidos pueden llevar al firewall a entrar en modo de mantenimiento, lo que requiere intervención manual para restaurar su funcionalidad.

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

- PAN-OS 11.0 en versiones anteriores a la versión 11.0.3.
- PAN-OS 10.2 en versiones anteriores a la versión 10.2.8.
- PAN-OS 10.1 en versiones anteriores a la versión 10.1.12.
- PAN-OS 9.1 en versiones anteriores a la versión 9.1.17.
- PAN-OS 9.0 en versiones anteriores a la versión 9.0.17-h4.

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-20: Stack-based Buffer Overflow.

CWE-476: NULL Pointer Dereference.

CVSS Base: **7.5**

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

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

CVE-2024-3384: vulnerabilidad en el software PAN-OS que permite a un atacante remoto reiniciar los firewalls PAN-OS al recibir paquetes de Windows New Technology LAN Manager (NTLM) desde servidores Windows. Los ataques repetidos eventualmente hacen que el firewall entre en modo de mantenimiento, lo que requiere intervención manual para restaurar su funcionamiento y volver a estar en línea.

Las versiones de PAN-OS afectadas son las siguientes:

- PAN-OS 10.0 versiones anteriores a la versión 10.0.12.
- PAN-OS 9.1 versiones anteriores a la versión 9.1.15-h1.

- PAN-OS 9.0 versiones anteriores a la versión 9.0.17.
- PAN-OS versiones anteriores a la versión 8.1.24.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-1286: Improper Validation of Syntactic Correctness of Input

CVSS Base: **7.5**

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

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

CVE-2024-3382: vulnerabilidad de fuga de memoria en el software PAN-OS que permite a un atacante enviar una ráfaga de paquetes manipulados a través del firewall, lo que eventualmente impide que el firewall procese el tráfico. Este problema solo afecta a los dispositivos de la serie PA-5400 que estén ejecutando el software PAN-OS con la función de Proxy SSL Forward habilitada.

Las versiones de PAN-OS afectadas por esta vulnerabilidad son:

- PAN-OS 11.1 versiones anteriores a la 11.1.2.
- PAN-OS 11.0 versiones anteriores a la versión 11.0.4.
- PAN-OS 10.2 versiones anteriores a la versión 10.2.7-h3

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-770: Allocation of Resources Without Limits or Throttling

CVSS Base: **7.5**

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

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

CVE-2024-3383: vulnerabilidad cuyo origen radica en cómo el software PAN-OS que procesa los datos recibidos de los agentes de Cloud Identity Engine (CIE) que permite la modificación de grupos de identificación de usuario (User-ID). Esto afecta el acceso de los usuarios a recursos de red donde los usuarios podrían ser inapropiadamente denegados o permitidos según las reglas de su Política de Seguridad existente.

Las versiones de PAN-OS son:

- PAN-OS 11.0 en versiones anteriores a la versión 11.0.3.
- PAN-OS 10.2 en versiones anteriores a la version 10.2.5.
- PAN-OS 10.1 en versiones anteriores a la version 10.1.11.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-282: Improper Ownership Management

CVSS Base: **7.4**

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

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

4. Mitigación / Solución

Como es habitual, para prevenir estas 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-2024-3385, Palo Alto recomienda:

- Actualizar a PAN-OS 11.0 a versión igual o superior a la versión 11.0.3
- Actualizar a PAN-OS 10.2 a versión igual o superior a la versión 10.2.8.
- Actualizar a PAN-OS 10.1 a versión igual o superior a la versión 10.1.12.
- Actualizar a PAN-OS 9.1 a versión igual o superior a la versión 9.1.17.
- Actualizar a PAN-OS 9.0 a versión igual o superior a la versión 9.0.17-h4.

Para corregir la vulnerabilidad CVE-2024-3384 Palo Alto recomienda:

- Actualizar PAN-OS 10.0 a versión igual o superior a la versión 10.0.12.
- Actualizar PAN-OS 9.1 a versión igual o superior a la versión 9.1.15-h1.
- Actualizar PAN-OS 9.0 a versión igual o superior a la versión 9.0.17.
- Actualizar PAN-OS 8.1 a versión igual o superior a la versión 8.1.24.

Para corregir la vulnerabilidad CVE-2024-3382 Palo Alto recomienda:

- Actualizar PAN-OS 11.1 a versión igual o superior a la versión 11.1.2.
- Actualizar PAN-OS 11.0 a versión igual o superior a la versión 11.0.4.
- Actualizar PAN-OS 10.2 a versión igual o superior a la versión 10.2.7-h3.

Para corregir la vulnerabilidad CVE-2024-3383 Palo Alto recomienda:

- Actualizar a PAN-OS 11.0 a versión igual o superior a la versión 11.0.3.
- Actualizar a PAN-OS 10.2 a versión igual o superior a la versión 10.2.5.
- Actualizar a PAN-OS 10.1 a versión igual o superior a la versión 10.1.11.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-3385.
- CVE-2024-3384.
- CVE-2024-3382.
- CVE-2024-3383.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY