Vulnerabilidades en ClearPass Policy Manager de Aruba

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

Aruba network ha publicado un aviso de seguridad corrigiendo **múltiples vulnerabilidades** que afectan al producto **Clearpass Policy Manager**, plataforma de políticas de acceso, la cual proporciona control en la red en base a roles y a dispositivos.

Entre las más significativas se encuentran **1 vulnerabilidad crítica** CVE-2023-50164 y **5 vulnerabilidades de severidad alta**, CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298, las cuales podrían permitir a usuarios remotos autenticados, ejecutar comandos arbitrarios como root en el host subyacente y comprometer el sistema al completo, representando, todas ellas, una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad en los sistemas que se puedan ver afectados por su explotación.

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

Las siguientes **versiones de software** ejecutadas por Clearpass Policy Manager y afectadas por estas vulnerabilidades, **han llegado al final de su ciclo de vida** y HPE Aruba no les aplicará parches:

- ClearPass Policy Manager 6.12.x: 6.12.0
- ClearPass Policy Manager 6.11.x: 6.11.6 e inferiores
- ClearPass Policy Manager 6.10.x: ClearPass 6.10.8 Hotfix Q4 2023 para problemas de seguridad e inferiores
- ClearPass Policy Manager 6.9.x: ClearPass 6.9.13 Hotfix Q4 2023 para problemas de seguridad y versiones inferiores

Cualquier otro producto de HPE Aruba Networking que no figure específicamente en la lista anterior, no se ve afectado por estas vulnerabilidades.

3. Análisis técnico

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

CVE-2023-50164: vulnerabilidad de inyección de comandos donde un atacante puede manipular los parámetros de carga de archivos para permitir la travesía de rutas y, bajo algunas circunstancias, esto puede llevar a la carga de un archivo malicioso que puede ser utilizado para realizar ejecución de código remoto. El impacto de esta vulnerabilidad en ClearPass Policy Manager no ha sido confirmado, pero la versión de Apache Struts ha sido actualizada para mitigarla. HPE Aruba Networking no tiene conocimiento de ninguna explotación maliciosa de esta vulnerabilidad.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 552: Files or Directories Accessible to External Parties

CVSS Base: **9.8**

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: Ningunos**
- **Interacción del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298: grupo de vulnerabilidades de Cross-Site Scripting (XSS) en la interfaz de gestión web de ClearPass Policy Manager que permite a los usuarios remotos autenticados ejecutar comandos arbitrarios en el host subyacente. Una explotación exitosa podría permitir a un atacante ejecutar comandos arbitrarios como root en el sistema operativo subyacente, lo que llevaría al compromiso completo del sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 552: Files or Directories Accessible to External Parties

CVSS Base: **7.2**

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

- **Vector de Ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos:** Altos
- **Interacción del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**

- **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.

HPE Aruba recomienda actualizar la plataforma ClearPass Policy a una de las siguientes versiones:

- ClearPass Policy Manager 6.12.x: 6.12.1 y superior.
- ClearPass Policy Manager 6.11.x: 6.11.7 y superior.
- ClearPass Policy Manager 6.10.x: 6.10.8 Hotfix Parche 8 Q1 2024 para problemas de seguridad y superiores.
- ClearPass Policy Manager 6.9.x: 6.9.13 Hotfix Parche 7 T1 2024 para problemas de seguridad y superiores.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-50164.
- CVE-2024-26294.
- CVE-2024-26295.
- CVE-2024-26296.
- CVE-2024-26297.
- CVE-2024-26298.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY