Vulnerabilidad en archivo OLE2 de ClamAV con impacto en productos Cisco

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

Cisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de **severidad alta**, en el analizador de formato de archivo **OLE2** de **ClamAV**. El identificador de este error, que podría permitir que un atacante remoto no autenticado generar una condición de denegación de servicio, es el CVE-2024-20290. El fallo podría suponer una amenaza de alta gravedad para productos de Cisco con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Por otra parte, el Equipo de Respuesta a Incidentes de Seguridad de Productos de Cisco (PSIRT) no tiene conocimiento de divulgación o uso malicioso de la vulnerabilidad descrita.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera el fallo destacado. Por lo que, para prevenir esta 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

- Secure Endpoint Connector for Windows versiones anteriores a la 7.5.17 (Feb 2024) 8.2.3.30119.
- Secure Endpoint Private Cloud versiones anteriores a la 3.8.0.

3. Análisis técnico

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

CVE-2024-20290: esta vulnerabilidad podría permitir a un atacante hacer que Cisco Secure Endpoint Connector para Windows, que se distribuye desde Cisco Secure Endpoint Private Cloud, entrara en un bucle y dejara de responder, dando lugar a una condición de DoS. Dicha vulnerabilidad se debe a una comprobación incorrecta de los valores de fin de cadena durante el análisis, lo que puede provocar una sobrelectura del búfer heap. Un atacante podría explotar esta vulnerabilidad enviando un archivo manipulado con contenido OLE2 para ser escaneado por ClamaV en un dispositivo afectado. Un exploit exitoso podría permitir al atacante causar que el proceso de escaneo de ClamAV termine, resultando en una condición DoS en el software afectado y consumiendo los recursos disponibles del sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-126: Buffer Over-read

CVSS Base: **7.5**

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 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 solucionar esta vulnerabilidad, Cisco recomienda a sus clientes a que actualicen a una versión de software adecuada:

- Para Secure Endpoint Connector for Windows, actualizar a la versión 7.5.17 (Feb 2024) 8.2.3.30119.
- Para Secure Endpoint Private Cloud, actualizar a 3.8.0 con conectores actualizados.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-20290.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY