Vulnerabilidades en Cisco Secure Client

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 avisos de seguridad para tratar **2 vulnerabilidades** de **severidad alta** en **Cisco Secure Client**. Los identificadores de estas vulnerabilidades son CVE-2024-20338, CVE-2024-20337. Su explotación supone una amenaza de alta gravedad para la confidencialidad de los sistemas que se vean afectados.

El Equipo de Respuesta a Incidentes de Seguridad de Productos de Cisco (PSIRT) no tiene conocimiento de divulgación o uso malicioso de las vulnerabilidades descritas.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. 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

Para la vulnerabilidad CVE-2024-20338:

- Dispositivos Cisco que ejecutan una versión vulnerable de Cisco Secure Client para Linux y tienen instalado el módulo ISE Posture.

Para la vulnerabilidad CVE-2024-20337:

- Cisco Secure Client para Linux.
- Cisco Secure Client para macOS.
- Cisco Secure Client para Windows.

3. Análisis técnico

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

CVE-2024-20337: vulnerabilidad que afecta al proceso de autenticación SAML de Cisco Secure Client posibilitando que un atacante remoto y no autenticado, lleve a cabo un ataque de inyección de retorno de carro y salto de línea (CRLF) contra un usuario. El origen de esta vulnerabilidad radica en una validación insuficiente de la entrada proporcionada por el usuario, de forma que, un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que haga clic en un enlace manipulado mientras establece una sesión VPN. Un exploit exitoso podría permitir que el atacante ejecute código de script arbitrario en el navegador o acceda a información sensible basada en el navegador, incluido un token SAML válido. El atacante podría luego usar el token para establecer una sesión VPN de acceso remoto con los privilegios del usuario afectado.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 93: Improper Neutralization of CRLF Sequences

CVSS Base: **8.2**

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

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

CVE-2024-20338: vulnerabilidad que afecta al módulo ISE Posture de Cisco Secure Client para Linux. Esta vulnerabilidad tiene su origen en el empleo de un elemento de ruta de búsqueda no controlado. Un atacante podría aprovechar esta vulnerabilidad copiando un archivo de biblioteca malicioso a un directorio específico en el sistema de archivos y persuadir a un administrador para que reinicie un proceso específico. Un exploit exitoso podría permitir al atacante ejecutar código arbitrario en un dispositivo afectado con privilegios de root.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 427: Uncontrolled Search Path Element

CVSS Base: **7.3**

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

- **Vector de ataque**: **Local**

- **Complejidad del ataque**: Baja
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: Requerida
- **Alcance**: **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.

Se aconseja actualizar a las siguientes versiones:

- Cisco Secure Client 4.10.04065 y posteriores actualizar a la versión 4.10.08025.
- Cisco Secure Client 5.1 actualizar a la versión 5.1.2.42.
- Cisco Secure Client para Linux versiones anteriores a la versión 5.1.2.42 actualizar a la versión 5.1.2.42.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-20337
- CVE-2024-20338.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY