Vulnerabilidad en Cisco Nexus Dashboard Controller

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

Cisco ha publicado aviso de seguridad para tratar **1 vulnerabilidad** de **severidad alta** que afecta a **Cisco Nexus Dashboard Fabric Controller.** El identificador de esta vulnerabilidad es CVE-2024-20348. 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 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

- Cisco NDFC (Cisco Nexus Dashboard Fabric Controler), versión 12.1.3b con una configuración predeterminada. Según informa Cisco, el alcance de esta vulnerabilidad se limita a las interfaces de red de datos y no puede ser explotada a través de las interfaces de gestión.

3. Análisis técnico

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

CVE-2024-20348: vulnerabilidad que afecta a la función Plug and Play (PnP) Out-of-Band (OOB) del controlador Cisco Nexus Dashboard Fabric, que tiene su origen en un servidor web de aprovisionamiento no autenticado. Un atacante podría explotar esta vulnerabilidad a través de solicitudes web directas al servidor de aprovisionamiento. La explotación exitosa podría permitir al atacante leer archivos sensibles en el contenedor PnP que podrían facilitar ataques adicionales en la infraestructura PnP.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 27: Path Traversal: 'dir/../../filename'

CVSS Base: **7.5**

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

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

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.

En el caso de la vulnerabilidad CVE-2024-20348, que afecta a la versión 12.1.3b de Cisco NDFC, se recomienda migrar a la versión 12.2.1, que se trata de una versión unificada que viene preempaquetada con Cisco Nexus Dashboard Release 3.1(1k).

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-20348.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY