BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

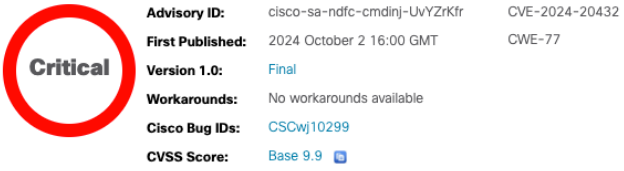
Boletín Nro.: 2024-44
Fecha de publicación: 03/10/2024
Tema: Vulnerabilidad Critica en Cisco NDFC y otros productos Cisco
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- La version Cisco NDFC 12.0 y superior.
- No afecta a la version Cisco NDFC 11.5 y superior (dentro de la rama).
- No afecta a los Cisco NDFC que tengan configurado el Storage Area Network (SAN).

Descripción

Se ha reportado una vulnerabilidad critica en el producto Cisco Nexus Dashboard Fabric Controller (NDFC), identificada como **CVE-2024-20432** con un score CVSSv3 9.9 y una criticidad critica.



Esta vulnerabilidad se debe a una autorización de usuario incorrecta y a una validación insuficiente de los argumentos de los comandos. Un atacante podría aprovechar esta vulnerabilidad enviando comandos creados a un punto final de API REST afectado o a través de la interfaz de usuario web. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en la CLI de un dispositivo administrado por Cisco NDFC con privilegios *de administrador de red*.

El **Cisco Nexus Dashboard Fabric Controller** es una solución de gestión y control para redes basadas en la arquitectura de Cisco Nexus. Proporciona visibilidad, automatización y control centralizados para entornos de red, especialmente aquellos que utilizan la tecnología de **Nexus** y la infraestructura de Data Center.

Es importante mencionar que esta vulnerabilidad no afecta a productos Cisco NDFC configurados para la implementación del controlador de almacenamiento en red (SAN - storage area network). Tampoco afecta al producto **Cisco NDFC** versión 11.5 y superior (dentro de la rama).

Para leer el informe de la alerta publicado por Cisco, puede encontrarlo en el siguiente enlace:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr

Existe un parche de seguridad que soluciona la vulnerabilidad **CVE-2024-20432**, recomendamos tomar medidas correctivas los mas pronto posible.

Además, del parche de seguridad ya mencionado, el equipo de CISCO hay proveido un set de actualizaciones para otras vulnerabilidades importantes en otros productos Cisco. De entre estas podemos destacar la vulnerabilidad identificada como CVE-2022-20824 con score CVSS 8.8 que afecta a los productos el Cisco FXOS y NX-OS.

La vulnerabilidad CVE-2022-20824 se activa debido a una validación de entrada incorrecta de valores específicos que se encuentran dentro de un mensaje del protocolo Cisco Discovery. El atacante podría enviar un paquete malicioso del protocolo Cisco Discovery a un dispositivo afectado y provocar un desbordamiento del búfer para ejecutar código o provocar una condición de denegación de servicio.

Debido a que el Protocolo de Discovery está habilitado de forma predeterminada a nivel global y en todas las interfaces de FXOS y NX-OS, CVE-2022-20824 afecta a numerosos productos, incluidos Nexus, Firepower, UCS y MDS.

Para ver la lista completa de las vulnerabilidades solucionadas y los parches de seguridad puede seguir el siguiente enlace:

https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir&limit=50#~Vulnerabilities

Cisco afirmó que no tiene conocimiento de “ningún anuncio público ni uso malintencionado o explotaciones activas” de las vulnerabilidades mencionadas anteriormente.

Solución

El equipo de Cisco ha publicado un parche de seguridad con la solución a la vulnerabilidad CVE-2022-20824 dentro de la versión Cisco NDFC 12.2.2.

Seguir el enlace para conseguir información de como actualizar su producto:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr#fs

Información adicional:

- https://securityonline.info/cve-2024-20432-cvss-9-9-cisco-nexus-dashboard-fabric-controller-exposed-to-rce/
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr
- https://www.securityweek.com/cisco-patches-critical-vulnerability-in-data-center-management-product/
- https://securityonline.info/cve-2022-20824-cisco-fxos-and-nx-os-arbitrary-code-execution-flaw/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com