Alerta de seguridad informática	9VSA-00112-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de enero de 2020
Última revisión	03 de enero de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a vulnerabilidades que afectan a sus productos.

Vulnerabilidades

CVE-2019-15999
CVE-2019-15983
CVE-2019-15978
CVE-2019-15979
CVE-2019-15980
CVE-2019-15981
CVE-2019-15982
CVE-2019-15984
CVE-2019-15985
CVE-2019-15975
CVE-2019-15976
CVE-2019-15977

Vulnerabilidad
CVE-2019-15999

Impacto
Una vulnerabilidad en el entorno de aplicación de Cisco Data Center Network Manager (DCNM) podría permitir que un atacante remoto autenticado obtenga acceso no autorizado a la Plataforma de aplicaciones empresariales JBoss (JBoss EAP) en un dispositivo afectado.

La vulnerabilidad se debe a una configuración incorrecta de la configuración de autenticación en JBoss EAP. Un atacante podría aprovechar esta vulnerabilidad autenticándose con una cuenta específica de bajos privilegios. Una explotación exitosa podría permitir al atacante obtener acceso no autorizado al JBoss EAP, que debería limitarse a las cuentas internas del sistema.

Productos Afectados
En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-unauth-access

---

Vulnerabilidad
CVE-2019-15983

Impacto
Una vulnerabilidad en la API SOAP de Cisco Data Center Network Manager (DCNM) podría permitir que un atacante remoto autenticado obtenga acceso de lectura a la información almacenada en un sistema afectado. Para aprovechar esta vulnerabilidad, un atacante necesitaría privilegios administrativos en la aplicación DCNM.

La vulnerabilidad existe porque la API SOAP maneja incorrectamente las entradas de entidad externa XML (XXE) al analizar ciertos archivos XML. Un atacante podría aprovechar esta vulnerabilidad insertando contenido XML malicioso en una solicitud de API. Una explotación exitosa podría permitir al atacante leer archivos arbitrarios del dispositivo afectado.

Productos Afectados
En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-xml-ext-entity

---

Vulnerabilidad
CVE-2019-15978
CVE-2019-15979

Impacto
Dos vulnerabilidades en los puntos finales API REST y SOAP de Cisco DCNM podrían permitir que un atacante remoto autenticado con privilegios administrativos en la aplicación DCNM inyecte comandos arbitrarios en el sistema operativo (SO) subyacente.

Las vulnerabilidades se deben a una validación insuficiente de la entrada proporcionada por el usuario a la API. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud diseñada a la API. Una explotación exitosa podría permitir a un atacante ejecutar comandos arbitrarios en el dispositivo con todos los privilegios administrativos.

Las vulnerabilidades no dependen una de otra; No se requiere la explotación de una de las vulnerabilidades para explotar la otra vulnerabilidad. Además, una versión de software que se ve afectada por una de las vulnerabilidades puede no verse afectada por la otra vulnerabilidad.

CVE-2019-15978: vulnerabilidad en la API REST de Cisco DCNM
CVE-2019-15979: vulnerabilidad en la API SOAP de Cisco DCNM

Productos Afectados
Estas vulnerabilidades afectan a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-comm-inject

---

Vulnerabilidad
CVE-2019-15980
CVE-2019-15981
CVE-2019-15982

Impacto
Múltiples vulnerabilidades en los puntos finales REST y SOAP API y en el Application Framework de Cisco Data Center Network Manager (DCNM) podrían permitir que un atacante remoto autenticado realice ataques transversales de directorio en un dispositivo afectado. Para explotar estas vulnerabilidades, un atacante necesitaría privilegios administrativos en la aplicación DCNM.

CVE-2019-15980: vulnerabilidad en la API REST de Cisco DCNM
CVE-2019-15981: vulnerabilidad en la API SOAP de Cisco DCNM
CVE-2019-15982: vulnerabilidad en el Application Framework de Cisco DCNM

Productos Afectados
Estas vulnerabilidades afectan a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-path-trav

---

Vulnerabilidad
CVE-2019-15984
CVE-2019-15985

Impacto
Múltiples vulnerabilidades en los puntos finales REST y SOAP API de Cisco Data Center Network Manager (DCNM) podrían permitir que un atacante remoto autenticado ejecute comandos SQL arbitrarios en un dispositivo afectado. Para explotar estas vulnerabilidades, un atacante necesitaría privilegios administrativos en la aplicación DCNM.

Las vulnerabilidades no dependen una de otra; No se requiere la explotación de una de las vulnerabilidades para explotar la otra vulnerabilidad. Además, una versión de software que se ve afectada por una de las vulnerabilidades puede no verse afectada por la otra vulnerabilidad.

CVE-2019-15984: vulnerabilidad en la API REST de Cisco DCNM
CVE-2019-15985: vulnerabilidad en la API SOAP de Cisco DCNM

Productos Afectados
Estas vulnerabilidades afectan a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-sql-inject

---

Vulnerabilidad
CVE-2019-15975
CVE-2019-15976
CVE-2019-15977

Impacto
Múltiples vulnerabilidades en los mecanismos de autenticación de Cisco Data Center Network Manager (DCNM) podrían permitir que un atacante remoto no autenticado omita la autenticación y ejecute acciones arbitrarias con privilegios administrativos en un dispositivo afectado.

CVE-2019-15975: vulnerabilidad en la API REST de Cisco DCNM
CVE-2019-15976: vulnerabilidad en la API SOAP de Cisco DCNM
CVE-2019-15977: vulnerabilidad en la interfaz de administración web de Cisco DCNM

Productos Afectados
Estas vulnerabilidades afectan a las versiones del software Cisco DCNM anteriores a la versión 11.3 (1) para Microsoft Windows, Linux y plataformas de dispositivos virtuales.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-auth-bypass

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.03 12:07:59 -03'00'