Cisco reveló una docena de errores que afectan su software Data Center Network Manager (DCNM), incluidos tres errores críticos de omisión de autenticación que exponen a los clientes empresariales a ataques remotos.

La compañía advierte que un atacante remoto puede omitir la autenticación de DCNM y realizar tareas con privilegios administrativos en un dispositivo afectado.

Las actualizaciones disponibles son muy importantes para los centros de datos empresariales creados con sus conmutadores basados en Nexus NX-OS. DCNM es un componente clave para automatizar las implementaciones de infraestructura de red basadas en NX-OS.

Cisco apunta a tres vulnerabilidades de omisión de autenticación separadas en un solo aviso. Están etiquetados como CVE-2019-15975, CVE-2019-15976 y CVE-2019-15977, las tres vulnerabilidades tienen una calificación de gravedad de 9.8 sobre 10, lo que significa que son problemas firmemente críticos.

> *«Los errores podrían permitir que un atacante remoto no autenticado omita la autenticación y ejecute acciones arbitrarias con privilegios administrativos en un dispositivo afectado»,* dijo Cisco.

Cisco explicó que las vulnerabilidades son independientes entre sí y que la explotación de una no es necesaria para explotar otra.

El primer error se debe a una clave de cifrado estático que se comparte entre las instalaciones. El problema reside en el punto final API REST de DCNM. Permite a un atacante utilizar la clave estática para generar un token de sesión válido y potencialmente realizar acciones a voluntad por medio de la API REST con privilegios administrativos.

La segunda vulnerabilidad proviene del mismo problema, sin embargo, se encuentra en el punto final API SOAP de DCNM. *«Una explotación exitosa podría permitir al atacante realizar acciones arbitrarias a través de la API SOAP con privilegios administrativos»*, advierte la

compañía.

El tercer error se debe a que Cisco agregó credenciales codificadas para la interfaz de usuario basada en la web, lo que podría permitir que un atacante acceda a una sección de la interfaz web y obtenga información confidencial de un dispositivo afectado.

Cisco afirma haber corregido las vulnerabilidades en las versiones 11.3 de Cisco DCNM Software y posteriores en Windows, Linux y plataformas de dispositivos virtuales.

Las vulnerabilidades fueron reportadas por Steven Seeley por medio de Zero Day Initiative de Trend Micro e iDefense, Accenture.

Seeley aconseja a los clientes parchear DCNM lo más pronto posible, y de no ser posible, desinstalar el software. Además, encontró tres errores de alta gravedad en los puntos finales API REST y SOAP en la función de Marco de Aplicación de DCNM. Estos errores podrían permitir que un atacante remoto autenticado realice ataques transversales de directorio en un dispositivo afectado.

Los errores afectan a Cisco DCNM antes de la versión 11.3 para Windows, Linux y plataformas de dispositivos virtuales. Los tres errores se debieron a una validación insuficiente de la entrada proporcionada por el usuario a las interfaces respectivas.

Dos errores adicionales que encontró en DCNM incluyeron una falla de inyección de comandos de alta gravedad en los puntos finales API REST y SOAP de DCNM, además de un problema de gravedad media en DCNM.