Contenido

Objetivo

Este documento es ayudar a resolver problemas/problemas del ssh de la resolución a los nexos 9000 después de la actualización de código.

Introducción

Antes de que buceo de profundidad en la causa del ssh publiquemos, es necesario saber sobre la vulnerabilidad siguiente (el modo CBC del servidor SSH cifra los algoritmos débiles habilitados y de SSH MAC habilitados) que afecta a la plataforma del nexo 9000.

CVE ID: CVE 2008-5161 (el modo CBC del servidor SSH cifra los algoritmos débiles habilitados y de SSH MAC habilitados)

Descripción del problema: Vulnerabilidad habilitada de las cifras del modo CBC del servidor SSH (cifras del modo CBC del servidor SSH habilitadas)

Configuran al servidor SSH para soportar el cifrado del Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje del texto simple del texto cifrado. Observe que este solamente las comprobaciones para plugs-in las opciones del servidor SSH y no marca para saber si hay versiones de software vulnerables.

Solución recomendada dada:
Inhabilite el cifrado de la cifra del modo CBC, y habilitelo modo de la cifra CTR o GCM cifrado.

Referencia
008-5161

Problema

Después de actualizar el código 7.0(3)I2(1) a los nosotros no podemos al nexo 9000 y el conseguir del ssh después del error

Solución

La razón detrás de incapaz a los nexos 9000 del ssh después de actualizar para cifrar 7.0(3)I2(1) y posterior, es Cihpers débil se inhabilita vía el arreglo CSCuv39937.

La solución a largo plazo para este problema es utilizar al cliente SSH actualizado/último que

hace las viejas cifras débiles inhabilitar.

La solución temporaria puede ser agregar las cifras débiles de siguiente detrás en el nexo 9000.

Observe que agregando las viejas cifras le apoyan van a utilizar las cifras y por lo tanto el riesgo de seguridad débiles.