Contenu

Objectif

Ce document est d'aider à dépanner/des questions ssh de résolution au Nexus 9000 après mise à niveau du code.

Introduction

Avant que nous plongée en eau profonde dans la cause du ssh émette, il est nécessaire de savoir la vulnérabilité suivante (le mode CBC de serveur de SSH chiffre les algorithmes faibles activée et de SSH de MAC activés) affectant la plate-forme du Nexus 9000.

ID CVE : CVE 2008-5161 (le mode CBC de serveur de SSH chiffre les algorithmes faibles activée et de SSH de MAC activés)

Description de question : Les chiffrements de mode CBC de serveur de SSH ont activé la vulnérabilité (les chiffrements de mode CBC de serveur de SSH activés)

Le serveur de SSH est configuré pour prendre en charge le bloc de chiffrement enchaînant le cryptage (CBC). Ceci peut permettre à un attaquant pour récupérer le message de plaintext du cryptogramme. Notez que ce module d'extension vérifie seulement les options du serveur de SSH et ne vérifie pas les versions de logiciel vulnérables.

Solution recommandée donnée :
Cryptage de chiffrement de mode CBC de débronchement, et mode de chiffrement CTR d'enable ou GCM
cryptage.

Référence
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161

Problème

Après évolution du code 7.0(3)I2(1) à nous ne pouvons pas au Nexus 9000 et obtenir de ssh après erreur

Solution

La raison derrière incapable au Nexus 9000 de ssh après évolution pour coder 7.0(3)I2(1) et plus tard, est Cihpers faible sont désactivées par l'intermédiaire de la difficulté CSCuv39937.

La solution à long terme pour ce problème est d'utiliser le client mis à jour/le plus tard de ssh qui fait désactiver de vieux chiffrements faibles.

La solution provisoire peut être d'ajouter des chiffrements faibles suivants de retour sur le Nexus 9000.

Notez qu'en ajoutant les vieux chiffrements vous soutiennent vont utiliser des chiffrements et par conséquent le risque de sécurité faibles.