# Содержание



# Цель

Этот документ должен помочь устранять неполадки/решать проблем ssh к Nexus 9000 после обновления кода.

# Введение

Прежде чем мы глубоко погрузимся в причину проблем ssh, необходимо знать о следующей уязвимости (Шифры Режима CBC Сервера SSH Включили и SSH, который Слабые Алгоритмы MAC Включили), влияние на платформу Nexus 9000.

ID CVE: CVE-2008-5161 (шифры режима CBC сервера SSH включили и SSH слабые алгоритмы MAC, включил),

Описание проблемы: Шифры Режима CBC Сервера SSH Включили Уязвимость (Шифры Режима CBC Сервера SSH Включили),

Сервер SSH настроен для поддержки шифрования Cipher Block Chaining (CBC). Это может позволить атакующему восстанавливать сообщение простого текста с шифрованного текста. Обратите внимание на то, что этот плагин только проверяет для опций сервера SSH и не проверяет для уязвимых версий программного обеспечения.

Данное рекомендуемое решение:
Отключите шифрование шифра режима CBC и включите CTR или режим шифра GCM шифрование.

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

# Проблема

После обновления кода к 7.0 (3) I2 (1) мы неспособны к ssh Nexus 9000 и получению ошибки слежения

# Решение

Причина позади неспособного к ssh Nexus 9000 после обновления к коду 7.0 (3) I2 (1) и позже, слабо, Cihpers отключены через CSCuv39937, исправляют.

Долгосрочное решение для этой проблемы состоит в том, чтобы использовать

обновленного/последнего клиента SSH, которому отключили старые слабые Шифры.

Временное решение может быть должно добавить после слабых шифров назад на Nexus 9000.

Обратите внимание на то, что путем добавления старых Шифров назад вы переходите к использованию слабые Шифры и следовательно угроза безопасности.