目次

目標

この資料は解決を助けることコードアップグレードの後で Nexus 9000 に/解決 ssh 問題です。

概要

ssh の原因への深い飛び込み発行する前に、Nexus 9000 プラットフォームに影響を与える次の脆弱性（SSH サーバ CBC はモード 有効に なるイネーブルになった及び SSH 弱い MAC アルゴリズムを暗号化します）について確認することは必要です。

CVE ID: CVE- 2008-5161（SSH サーバ CBC はモード 有効に なるイネーブルになった及び SSH 弱い MAC アルゴリズムを暗号化します）

問題説明: SSH サーバ CBC モード暗号イネーブルになった脆弱性（有効に なる SSH サーバ CBC モード暗号）

SSH サーバは Cipher Block Chaining（CBC）暗号化をサポートするために設定されます。 これは攻撃者が暗号文からのプレーンテキスト メッセージを回復 することを可能にするかもしれません。 このプラグインが SSH サーバのオプションがあるようにのためにだけ確認し、脆弱 な ソフトウェア バージョンがあるように確認しないことに注目して下さい。

提供される推奨される ソリューション:
CBC モード暗号暗号化をディセーブルにし、CTR または GCM 暗号モード 有効に して下さい 暗号化。

参照
008-5161

問題

7.0(3)I2(1) へのコードをアップグレードした後でエラーの後で ssh Nexus 9000 および得ることにないです

解決策

7.0(3)I2(1) およびそれ以降をコードするアップグレードした後で ssh Nexus 9000 へのないの後ろの原因は弱い Cihpers です CSCuv39937 修正によって無効です。

この問題のための長期ソリューションはディセーブルにされる古く弱い暗号がある更新済を/最も遅く SSH クライアントを使用することです。

一時ソリューションは Nexus 9000 で続く弱い暗号を追加することである場合もあります。

追加によって古い暗号が弱い暗号およびそれ故にセキュリティリスクをことを使用する行っている支持することに注目して下さい。