2017 年 2 月 1 日

伊藤忠テクノソリューションズ株式会社

Cisco Nexus-OS に関する脆弱性について

Cisco Nexus-OS の SSH 実装に脆弱性が存在する事が判明しました。この脆弱性は、SSH 接続のネゴシエーションパラメータの取扱不備により発生します。
リモート攻撃者がこの脆弱性を利用し成功した場合、AAA 認証をすり抜けて対象機器でコマンド実行が出来てしまう可能性があります。

■脆弱性の詳細情報

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-nxaaa

■対象製品

以下の製品で、AAA の認証によって、IPv4 又は IPv6 の SSH アクセスできるように設定されている場合、この脆弱性の影響を受ける可能性があります。

- Multilayer Director Switches
- Nexus 1000V Series Switches
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 4000 Series Switches
- Nexus 5000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches NX-OS mode

■対象ソフトウェアバージョン

対象ソフトウェアのバージョンについては、以下の URL を参照してください。

- Nexus 1000：CSCuw79754
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuw79754
- Nexus 3000：CSCum35502
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCum35502
- Nexus 3500：CSCum35502
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCum35502
- Nexus 4000：CSCuw78669
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuw78669
- Nexus 5000：CSCux88492
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCux88492
- Nexus 2000, 5500, 5600, 6000：CSCux88492
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCux88492
- Nexus 7000, 7700：CSCum35502
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCum35502
- Nexus 9000 NX-OS Mode：CSCum35502
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCum35502
- MDS 9000：CSCum35502
  - https://bst.cloudapps.cisco.com/bugsearch/bug/CSCum35502

対処方法

恒久対策として、修正ソフトウェアへのバージョンアップを行ってください。

■修正ソフトウェアの入手方法

以下のサイトから入手可能です（事前にアカウント登録必要）

http://www.cisco.com/cisco/software/navigator.html

お問い合わせは、弊社担当営業までお願いいたします。

以　上