2016 年 12 月 6 日

伊藤忠テクノソリューションズ株式会社

Cisco Nexus-OS の DHCPv4 に関する脆弱性について

Cisco Nexus-OS ソフトウェアでの DHCPv4 リレーエージェント処理に脆弱性が存在する事が判明しました。
この脆弱性を利用して、リモートの攻撃者による DHCP プロセスの中断またはサービス拒否（DoS）状態が引き起こされる可能性があります。

■脆弱性の詳細情報

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp2

■対象製品

この脆弱性は以下の製品で DHCPv4 プロセスが有効であり、DHCPv4 のリレーエージェントとして構成されたデバイスのみに影響します。

- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform 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 in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in NX-OS mode

■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