2016 年 12 月 2 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 Border Gateway Protocol（BGP）に脆弱性が存在する事が判明しました。この脆弱性は、受信した BGP メッセージのチェックの不備により発生します。
リモート攻撃者による特殊な偽造 BGP パケットが送りつけられる事に起因して、対象機器のリロードが発生しサービス拒否（DoS）状態 とな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-bgp

■対象製品
以下の機器で BGP を設定している場合、この脆弱性の影響を受ける可能性があります。

・Nexus 1000v Series Switches
・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 ACI mode
・Nexus 9000 Series Switches in 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。

Cisco Nexus 1000 Series Switches：CSCux11417

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCux11417

Cisco Nexus 3000, 3500, 2000, 5000, 5500, 6000, 7000, 9000 and 9000-ACI Series Switches：CSCuq77105

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuq77105

■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