2017 年 2 月 21 日

伊藤忠テクノソリューションズ株式会社

Cisco Nexus シリーズの OS に関する脆弱性について

Cisco Nexus シリーズの OS の DHCP リレーエージェントまたはスマートリレーエージェントに脆弱性が存在する事が判明しました。この脆弱性は、DHCPv4 Offer パケットの取り扱いプロセス不備により発生します。特殊な偽造 DHCPv4 Offer パケットを受信すると、機器がクラッシュまたは、Denial of Service (DoS) とよばれるサービス妨害を受ける可能性があります。

■脆弱性の詳細情報

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp1

■対象製品およびバージョン

以下の製品で、DHCP の設定を行っている場合にこの脆弱性の影響を受ける可能性があります。

- Nexus 2000 Series Fabric Extenders
- 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 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。

脆弱性修正バージョン：

- Nexus 2000, 5500, 5600, 6000：CSCus21693

  7.1 及びそれ以前：7.1(4)N1(1)

  7.2：7.2(2)N1(1)

  7.3：7.3(0)N1(1)

- Nexus 5000：CSCus21693

  5.2 及びそれ以前：5.2(1)N1(9a)

- Nexus 7000, 7700：CSCuq24603

  6.2 及びそれ以前：7.2(2)D1(1)

  7.2：7.2(2)D1(1)

  7.3：7.3(1)D1(1)

- Nexus 9000 ACI Mode：CSCut76171

  11.0：11.1(1j)

  11.1：11.1(1j)

  11.2：脆弱性に該当しない

- Nexus 9000 NX-OS Mode：CSCur93159

  7.0 及びそれ以前：7.0(3)I4(1)

■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