

Cisco IOS/IOS XE、DHCP リモートコード実行の脆弱性について

Cisco IOS 及び IOS XE の DHCP Relay 機能に脆弱性があり、リモートから認証を受けずに該当機器上で任意プログラムの実行や、機器をリモート操作する可能性のあることが判明しました。

この脆弱性は、特殊な偽造 DHCP Version4 (DHCPv4) パケットを受信しつづけることによるバッファ・オーバーフローに起因します。

■脆弱性の詳細情報

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp>

■対象製品およびバージョン

IOS または IOS XE が動作し、DHCP Relay Agent 機能が設定されている機器。

■対処方法

恒久対策として、下記修正ソフトウェアにバージョンアップを行ってください。

使用しているソフトウェアがこの脆弱性に該当するかどうかを確認するには、下記の Cisco IOS Software Checker をご使用ください。

<https://tools.cisco.com/security/center/selectIOSVersion.x>

■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