2016 年 11 月 21 日

伊藤忠テクノソリューションズ株式会社

Cisco IOS/IOS-XE ソフトウェアに関する脆弱性について

Cisco IOS/IOS-XE ソフトウェアの Internet Key Exchange Version 1 (IKEv1)のパケットをフラグメント化するコード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、未承認のリモート攻撃者は、機器のメモリを枯渇させたり、再起動することが可能になります。

■脆弱性の詳細情報

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1

■対象製品

IOS/IOS-XE ソフトウェア製品全般

この脆弱性は、以下 2 つの条件に合致する場合に影響を受けます。

1．IKEv1 のフラグメンテーションが有効化されている。

通常、IKEv1 フラグメンテーションは無効（disable）となっているため、以下のコマンドを実行しステータスを確認してください。

```
router#show running-config | include crypto isakmp fragmentation
 crypto isakmp fragmentation      ←有効となっています。
router#
```

2．IOS か IOS XE が実行されていて、IKEv1 に基づくいずれかのタイプの VPN 用に設定されている。

IKEv1 は、以下の VPN タイプを含む、多くの機能で使用されます。

- LAN 間 VPN (LAN-to-LAN VPN)
- リモート アクセス VPN（SSL VPN を除く）
- Dynamic Multipoint VPN（DMVPN）

・FlexVPN

・Group Encrypted Transport VPN（GETVPN）

IKEv1 がデバイスに設定されているかどうかを確認するには、show ip sockets または　show udp EXEC コマンドを使用します。表示された内容においてデバイスの UDP ポート 500 または 4500 が開放されている場合、そのデバイスは IKE パケットを処理しているので VPN 用に設定されていると考えられます。

■対象ソフトウェアバージョン

対象バージョンのリストは公開されていませんので、下記 Tool を使って使用の有無を確認してください。

Cisco IOS Software Checker

http://tools.cisco.com/security/center/selectIOSVersion.x

■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。

【ワークアラウンド】

IKEv1 フラグメンテーションを無効化する

router#no crypto isakmp fragmentation

■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