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 ASA 製品のセキュリティモジュールに関する脆弱性について

Cisco ASA 製品の CX セキュリティモジュール（Context-Aware Security）に脆弱性が存在する事が判明しました。この脆弱性は、IP フラグメントパケットの不適切な処理により発生します。リモートの攻撃者が不正なパケットを CX モジュールに送信し続けることにより、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-20170125-cas

■対象製品

ASA CX Context-Aware Security モジュールを使用している全てのバージョン

■対処方法

本脆弱性に対する回避策はありませんので、以下の緩和策を実行することにより、脆弱性が晒されるのを制限することが可能です。

・ ASA で受信した全ての IP フラグメントパケットを破棄する設定

```
ASA# conf t
ASA(config)# fragment chain 1
ASA(config)# exit
```

なお、この設定を設定した場合、ASA CX モジュール専用のトラフィックだけでなく、ASA を通過する全てのユーザトラフィックに影響します。
またこの設定により全ての IP フラグメントが ASA 上で破棄されます。

■修正ソフトウェアの入手方法

CX モジュールに対するソフトウェアメンテナンスは終了しているため、本脆弱性に対する修正バージョンは、提供されません。

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