

2017年11月1日

伊藤忠テクノソリューションズ株式会社

## Cisco ASA ソフトウェアに関する脆弱性について

Cisco ASA ソフトウェアの IPSec パケットの処理に関して脆弱性が存在する事が判明しました。この脆弱性は、不正な IPSec パケットを不適切に解析する事に起因します。リモートの攻撃者が不正な IPSec パケットを対象機器に送信し続ける事により、サービス停止 (DoS) 状態を引き起こす可能性があります

### ■ 本件の詳細情報

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-ipsec>

### ■ 対象製品

- Cisco ASA 1000V Cloud Firewall
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance

また ASA で 下記 IPSec VPN の終端設定をしている場合、本脆弱性に該当する恐れがあります。

- LAN-to-LAN IPsec VPN
- Remote access VPN using the IPsec VPN client
- Layer 2 Tunneling Protocol (L2TP)-over-IPsec VPN connections
- Internet Key Exchange Version 2 (IKEv2) AnyConnect

## ■ 対処方法

修正されたソフトウェアへのバージョンアップをお願いします。

利用バージョン	修正バージョン
9.0 以前	9.1(7.8) 以降※
9.0	9.1(7.8) 以降※
9.1	9.1(7.8) 以降※
9.2	9.2(4.15) 以降
9.3	9.4(4) 以降※
9.4	9.4(4) 以降
9.5	9.5(3.2) 以降
9.6	9.6(2) 以降へ
9.7	該当しません
9.8	該当しません

※9.1 より前、及び 9.3 の Cisco ASA ソフトウェアリリースは、ソフトウェアメンテナンスが終了しているため、サポートされているリリースに移行する必要があります。

## ■ 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