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 ソフトウェアの SSL/TLS に関する脆弱性について

Cisco ASA ソフトウェアの SSL または TLS パケット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、細工された SSL または TLS パケットの不適切な解析に起因します。リモートの攻撃者が細工したパケットを送信し続けることにより、再立ち上げ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-tls

■対象製品

次の製品で動作する Cisco ASA ソフトウェアが影響を受けます。

- 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

■対処方法

不具合が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いたします。

利用バージョン	修正バージョン
9.0 以前	8.4(7.31)または 9.1(7)以上 ※
9.0	9.0(4.39)以上 ※
9.1	9.1(7)以上
9.2	9.2(4.6)以上
9.3	9.3(3.8)以上※
9.4	9.4(2)以上
9.5	9.5(2)以上
9.6	影響を受けません
9.7	影響を受けません
9.8	影響を受けません

※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