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 クライアントレス SSL VPN 機能に関する脆弱性について

Cisco ASA 製品のクライアントレス SSL VPN 機能に脆弱性が存在する事が判明しました。この脆弱性は、クライアントレス SSL VPN 機能の Common Internet Filesystem（CIFS）コード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送信し続けることにより、機器のリロード、または遠隔操作を実行す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-20170208-asa

■対象製品

下記製品にて、クライアントレス SSL VPN ポータルが有効な場合にこの脆弱性の影響を受けます。

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco ASA for Firepower 9300 Series
- Cisco ASA for Firepower 4100 Series
- Cisco ISA 3000 Industrial Security Appliance

■対処方法

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。

- 9.0 未満　9.1(7.13)以上 ※1
- 9.0　　9.1(7.13)以上 ※1
- 9.1　　9.1(7.13)以上

・ 9.2　　9.4(4)以上 ※2
・ 9.3　　9.4(4)以上 ※1
・ 9.4　　9.4(4)以上
・ 9.5　　9.6(2.10)以上 ※2
・ 9.6　　9.6(2.10)以上
・ 9.7　　影響を受けません

※1 9.1 および Cisco 9.3 より前のバージョンは、ソフトウェア保守が終了しているため、保守提供中のバージョンに移行する必要があります。

※2 Cisco ASA 9.2 および 9.5 での修正バージョンは、2017 年 4 月にリリースされます。

■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