2017 年 2 月 6 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 ソフトウェアのアイデンティティファイアウォール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、コード領域のバッファオーバーフローに起因します。この脆弱性を利用してリモート攻撃者がシステムの再起動やリモートでのコマンド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-20161019-asa-idfw

■対象製品及びバージョン

以下の製品のうち、Cisco ASA ソフトウェアのアイデンティティファイアウォール機能として、NetBIOS が有効なプロービングで設定されている場合に影響を受けます。

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco Catalyst 6500 Series/7600 Series ASA Services Module
- Cisco ASA 1000V Cloud Firewall
- 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

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。

影響のないバージョン

・　7.2　影響を受けません
・　8.0　影響を受けません
・　8.1　影響を受けません
・　8.2　影響を受けません
・　8.3　影響を受けません

影響を受けるバージョン

・　8.4　9.1(7.11)以上
・　8.5　9.1(7.11)以上
・　8.6　9.1(7.11)以上
・　8.7　9.1(7.11)以上
・　9.0　9.0(4.42)以上
・　9.1　9.1(7.11)以上
・　9.2　9.2(4.17)以上
・　9.3　9.3(3.11)以上
・　9.4　9.4(3.11)以上
・　9.5　9.5(3.1)以上
・　9.6　9.6(2.1)以上

※なお Cisco ASA ソフトウェアのバージョン 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7 はメーカー保守が終了しているため、現在保守されているバージョン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