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 DNS に関する脆弱性について

Cisco ASA ソフトウェアの DNS 要求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、細工された DNS 応答メッセージの不適切な処理に起因します。リモートの攻撃者が ASA からの DNS 要求を受けて細工された返答を送信し続けることにより、対象機器がサービス停止（DoS）状態やローカル DNS キャッシュ情報が破損される可能性があります

■本件の詳細情報

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns

■対象製品

以下の機器上で、ASA ソフトウェアが稼働する場合に影響を受ける可能性があります。

- 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

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(7.12)以降※
9.0	9.1(7.12)以降※
9.1	9.1(7.12)以降※
9.2	9.2(4.18)以降
9.3	9.4(3.12)以降※
9.4	9.4(3.12)以降
9.5	9.5(3.2)以降
9.6	9.6(2.2)以降
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