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 Firepower のマルチキャストプロトコルに関する脆弱性について

Cisco Firepower の Pragmatic General Multicast（PGM）プロトコル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、PGM プロトコルパケットの不適切な処理に起因します。リモートの攻撃者が細工された PGM パケットを対象機器の検索エンジンに送信し続ける事により、Snort プロセスが再起動し、通信内容の横取りや通信のドロップが発生し、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-fpsnort

■対象製品

- Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services
- Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls
- Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances
- Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances
- Firepower 4100 Series Security Appliances
- FirePOWER 7000 Series Appliances
- FirePOWER 8000 Series Appliances
- Firepower 9300 Series Security Appliances
- FirePOWER Threat Defense for Integrated Services Routers (ISRs)

- Industrial Security Appliance 3000
- Sourcefire 3D System Appliances
- Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware

■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。

- 5.4.0.10
- 5.4.1.9
- 6.0.1.3
- 6.1.0
- 6.2.0

■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