2016 年 12 月 2 日

伊藤忠テクノソリューションズ株式会社

Cisco FirePower に関する脆弱性について

Cisco FirePower System Software の検出エンジンに脆弱性が存在する事が判明しました。この脆弱性は、HTTP パケットストリームの不適切な処理により発生します。

リモート攻撃者が FirePower 上で検出エンジンに対し、細工した HTTP パケットストリームを送信した際、Snort プロセスの予期しない再起動が発生し、サービス拒否（DoS）状態 となる可能性があります。

■脆弱性の詳細情報

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-fpsnort

■対象製品及びバージョン

以下製品のうち、Software の Version が 5.4.1.5, 6.0, 6.0.0.1 で稼働しているデバイスが影響をうけます。

- Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services
- 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)
- Sourcefire 3D System Appliances
- Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware

■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。

- Firepower System Software
- 5.4.1.6
- 6.0.1
- 6.1.0

■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