お知らせ

2020年12月3日
内閣サイバーセキュリティセンター

Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について

Fortinet製FortiOSのSSL VPN機能には、外部から当該機器内にある任意のファイルを読み取ることが可能な脆弱性(CVE-2018-13379)が存在します。

2020年11月19日以降、本脆弱性の影響が考えられるVPN機器のIPアドレスがWebサイトで公開されています[1]。

本日、内閣サイバーセキュリティセンターは、公開情報を基に情報収集・分析し、確認した重要インフラ事業者等関連のVPN装置(218事業者、4,954 IPアドレス)について、所管省庁に対して注意喚起を行いました。

参考URL
- PSIRT Advisory FG-IR-18-384-FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests-(Fortinet)
  https://www.fortiguard.com/psirt/FG-IR-18-384
- CVE-2018-13379 に関するアップデート(Fortinet)
  https://www.fortinet.co.jp/blog/business-and-technology/update-regarding-cve-2018-13379.html
- Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性(CVE-2018-13379) の影響を受けるホストに関する情報の公開について(JPCERT/CC)
  https://www.jpcert.or.jp/newsflash/2020112701.html
- 複数の SSL VPN 製品の脆弱性に関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2019/at190033.html

本件に関する連絡先
内閣サイバーセキュリティセンター
電話番号03-5253-2111(代表)
重要インフラ第2グループ

[1] *Bleeping Computer「Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs(2020/11/22)」、https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/ (2020/12/3閲覧)*