2022 年 12 月 13 日
株式会社ネットワールド

FortiOS - sslvpnd でのヒープベースのバッファ オーバーフローについて

Fortinet 社の PSIRT(Product Security Incident Response Team)より Critical として、
以下の情報が公開されましたので、以下の通りご報告させていただきます。

概要：
FortiOS SSL-VPN のヒープベースのバッファ オーバーフローの脆弱性［CWE-122］により、
認証されていないリモートの攻撃者が特別に細工されたリクエストを介して任意のコード
またはコマンドを実行できる可能性があります。

CVE ID：
CVE-2022-42475

影響：
許可されていないコードまたはコマンドを実行する

Exploitation Status:
フォーティネットは、この脆弱性が実際に悪用された例を認識しており、
次の侵害の兆候にを確認することをお客様に推奨しています。

次の複数のログ エントリ：
Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11
received, Backtrace: [...]“

ファイルシステムに次のアーティファクトが存在します。
/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/libipudp.so
/data/lib/libjepg.so
/var/.sslvpnconfigbk
/data/etc/wxd.conf
/flash

FortiGate から疑わしい IP アドレスへの接続:

188.34.130.40:444

103.131.189.143:30080,30081,30443,20443

192.36.119.61:8443,444

172.247.168.153:8033

回避策:

SSL-VPN を無効にします。

影響を受ける製品：

FortiOS バージョン 7.2.0 から 7.2.2

FortiOS バージョン 7.0.0 から 7.0.8

FortiOS バージョン 6.4.0 から 6.4.10

FortiOS バージョン 6.2.0 から 6.2.11

FortiOS バージョン 6.0.0 から 6.0.15

FortiOS バージョン 5.6.0 から 5.6.14

FortiOS バージョン 5.4.0 から 5.4.13

FortiOS バージョン 5.2.0 から 5.2.15

FortiOS バージョン 5.0.0 から 5.0.14

FortiOS-6K7K バージョン 7.0.0 から 7.0.7

FortiOS-6K7Kバージョン 6.4.0 から 6.4.9

FortiOS-6K7K バージョン 6.2.0 から 6.2.11

FortiOS-6K7K バージョン 6.0.0 から 6.0.14

ソリューション：

FortiOS バージョン 7.2.3 以降にアップグレードしてください

FortiOS バージョン 7.0.9 以降にアップグレードしてください

FortiOS バージョン 6.4.11 以降にアップグレードしてください

FortiOS バージョン 6.2.12 以降にアップグレードしてください

FortiOS-6K7K バージョン 7.0.8 にアップグレードしてください

FortiOS-6K7K バージョン 6.4.10 以降にアップグレードしてください

FortiOS-6K7K バージョン 6.2.12 以降にアップグレードしてください

FortiOS-6K7K バージョン 6.0.15 以降にアップグレードしてください

URL：

https://fortiguard.fortinet.com/psirt/FG-IR-22-398

以上