文書管理番号：SCSK- 23036233
2023 年 6 月 15 日

お客様各位

SCSK 株式会社
ネットワークセキュリティ事業本部
カスタマーサポート部

FortiOS　SSL-VPN の脆弱性(CVE-2023-27997)について

平素より格別のご高配を賜り、厚く御礼を申し上げます。
標題の件について、弊社から販売させて頂きました Fortinet 製品について、
FortiOS および FortiProxy の SSL-VPN 機能におけるヒープベースのバッファーオーバーフローの脆弱性（CVE-2023-27997）の影響を受ける場合がございます。本脆弱性の内容について、下記の通りご報告申し上げます。

敬具

記

1. 事象

対象の FortiOS および FortiProxy の SSL-VPN 機能においてヒープベースのバッファーオーバーフローの脆弱性（CVE-2023-27997） があり、本脆弱性が悪用されると、認証されていない遠隔の第三者によって細工したリクエストを送信され、任意のコードやコマンドを実行される危険性があります。

２．対象

・FortiOS-6K7K バージョン 7.0.10
・FortiOS-6K7K バージョン 7.0.5
・FortiOS-6K7K バージョン 6.4.12
・FortiOS-6K7K バージョン 6.4.10
・FortiOS-6K7K バージョン 6.4.8
・FortiOS-6K7K バージョン 6.4.6
・FortiOS-6K7K バージョン 6.4.2
・FortiOS-6K7K バージョン 6.2.9 から 6.2.13 まで
・FortiOS-6K7K バージョン 6.2.6 から 6.2.7 まで
・FortiOS-6K7K バージョン 6.2.4
・FortiOS-6K7K バージョン 6.0.12 から 6.0.16 まで

・FortiOS-6K7K バージョン 6.0.10
・FortiProxy バージョン 7.2.0 から 7.2.3 まで
・FortiProxy バージョン 7.0.0 から 7.0.9 まで
・FortiProxy バージョン 2.0.0 から 2.0.12 まで
・FortiProxy 1.2 全バージョン
・FortiProxy 1.1 全バージョン
・FortiOS バージョン 7.2.0 から 7.2.4 まで
・FortiOS バージョン 7.0.0 から 7.0.11 まで
・FortiOS バージョン 6.4.0 から 6.4.12 まで
・FortiOS バージョン 6.2.0 から 6.2.13 まで
・FortiOS バージョン 6.0.0 から 6.0.16 まで

3．恒久対策

本脆弱性を回避する方法は以下バージョンへのアップデートとなります。

・FortiOS-6K7K バージョン 7.0.12 あるいはそれ以降
・FortiOS-6K7K バージョン 6.4.13 あるいはそれ以降
・FortiOS-6K7K バージョン 6.2.15 あるいはそれ以降
・FortiOS-6K7K バージョン 6.0.17 あるいはそれ以降
・FortiProxy バージョン 7.2.4 あるいはそれ以降
・FortiProxy バージョン 7.0.10 あるいはそれ以降
・FortiOS バージョン 7.4.0 あるいはそれ以降
・FortiOS バージョン 7.2.5 あるいはそれ以降
・FortiOS バージョン 7.0.12 あるいはそれ以降
・FortiOS バージョン 6.4.13 あるいはそれ以降
・FortiOS バージョン 6.2.14 あるいはそれ以降
・FortiOS バージョン 6.0.17 あるいはそれ以降

4．回避策

SSL-VPN 機能の無効化により回避できます。
SSL-VPN 機能を使用していない場合は無効に設定してください。

最新情報は下記 URL をご参照ください。
https://www.fortiguard.com/psirt/FG-IR-23-097

以上