文書管理番号：SCSK- 23047801
2023 年 7 月 14 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　バッファオーバーフローの脆弱性(CVE-2023-33308)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 において、スタックベースのバッファオーバーフローの脆弱性（CVE-2023-33308）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

FortiOS および FortiProxy には、スタックベースのオーバーフローの脆弱性があり、遠隔の攻撃者により細工されたパケットが、プロキシポリシーまたは SSL ディープパケットインスペクションが使用されている際に、プロキシモードのファイアウォールポリシーに到達することで、任意のコードまたはコマンドを実行される可能性があります。

２．対象製品バージョン

・FortiOS バージョン 7.2.0 から 7.2.3 まで
・FortiOS バージョン 7.0.0 から 7.0.10 まで
・FortiProxy バージョン 7.2.0 から 7.2.2 まで
・FortiProxy バージョン 7.0.0 から 7.0.9 まで

影響を受けない製品バージョン

・FortiOS 6.4 全バージョン
・FortiOS 6.2 全バージョン
・FortiOS 6.0 全バージョン
・FortiProxy 2.x 全バージョン
・FortiProxy 1.x 全バージョン

３．対策

以下のバージョンにアップグレードして下さい。

FortiOS バージョン 7.2.4 以降、7.0.11 以降

FortiProxy バージョン 7.2.3 以降、7.0.10 以降

最新の情報は以下の PSIRT Advisories よりご確認ください。

https://www.fortiguard.com/psirt/FG-IR-23-183

※日本語による情報は、英語による原文の非公式な翻訳となります。

もし、英語原文との間で内容の齟齬がある場合、英語原文が優先されます。

以上