2023 年 6 月 13 日
株式会社ネットワールド

FortiOS および FortiProxy - sslvpn 事前認証における ヒープ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 および FortiProxy 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、リモート攻撃者が特別に作成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-2023-27997

影響：
不正なコードまたはコマンドを実行する

影響を受ける製品：
FortiOS バージョン 7.2.0 ～ 7.2.4
FortiOS バージョン 7.0.0 ～ 7.0.11
FortiOS バージョン 6.4.0 ～ 6.4.12
FortiOS バージョン 6.2.0 ～ 6.2.13
FortiOS バージョン 6.0.0 ～ 6.0.16

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 ～ 6.2.13
FortiOS-6K7K バージョン 6.2.6 ～ 6.2.7
FortiOS-6K7K バージョン 6.2.4
FortiOS-6K7K バージョン 6.0.12 ～ 6.0.16
FortiOS-6K7K バージョン 6.0.10以上
※FortiGate6000系、7000系となります。

FortiProxy バージョン 7.2.0 ～ 7.2.3
FortiProxy バージョン 7.0.0 ～ 7.0.9
FortiProxy バージョン 2.0.0 ～ 2.0.12
FortiProxy 1.2 のすべてのバージョン
FortiProxy 1.1 のすべてのバージョン

回避策：
SSL-VPN 機能の無効化にて回避可能でございます。しかしながら、正式な対策としましては、
対策済 FOS のご利用をお願いいたします。

https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/869159/ssl-vpn-best-practices

To disable SSL VPN in the CLI:
config vpn ssl settings
set status disable
end

ソリューション：
FortiOS バージョン 7.4.0 以降にアップグレードしてください
FortiOS バージョン 7.2.5 以降にアップグレードしてください
FortiOS バージョン 7.0.12 以降にアップグレードしてください
FortiOS バージョン 6.4.13 以降にアップグレードしてください
FortiOS バージョン 6.2.14 以降にアップグレードしてください
FortiOS バージョン 6.0.17 以降にアップグレードしてください

FortiOS-6K7K バージョン 7.0.12 以降にアップグレードしてください
FortiOS-6K7K バージョン 6.4.13 以降にアップグレードしてください
FortiOS-6K7K バージョン 6.2.15 以降にアップグレードしてください
FortiOS-6K7K バージョン 6.0.17 以降にアップグレードしてください

FortiProxy バージョン 7.2.4 以降にアップグレードしてください
FortiProxy バージョン 7.0.10 以降にアップグレードしてください
FortiProxy バージョン 2.0.13 以降にアップグレードしてください

URL：
https://www.fortiguard.com/psirt/FG-IR-23-097

以上