

2024年2月16日

株式会社ネットワーク

FortiOS - sslvpn でのアウトオブバウンド書き込みについて

このたびFortinet社が提供するFortiGate製品にて以下脆弱性があることがわかりましたので、以下の通りご報告させていただきます。

CVE ID :

CVE-2024-21762

1. 対象製品について

SSL VPN サービスが有効になっている全てのFortiGate

【対象 OS】

FortiOS v7.4.0 から v7.4.2

FortiOS v7.2.0 から v7.2.6

FortiOS v7.0.0 から v7.0.13

FortiOS v6.4.0 から v6.4.14

FortiOS v6.2.0 から v6.2.15

FortiOS v6.0.0 すべてのバージョン

FortiProxy v7.4.0 から 7.4.2

FortiProxy v7.2.0 から 7.2.8

FortiProxy v7.0.0 から 7.0.14

FortiProxy v2.0.0 から 2.0.13

FortiProxy v1.2.0 すべてのバージョン

FortiProxy v1.1.0 すべてのバージョン

FortiProxy v1.0.0 すべてのバージョン

2. 概要について

FortiOS SSL-VPNに境界外書き込みの脆弱性 [CWE-787] が内在し、リモートの攻撃者が、特別に細工されたHTTPリクエストを経由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。

3. 対策について

本脆弱性の影響を受けないファームウェアへのアップグレードをお願いいたします。

影響を受けないファームウェアは以下となります。

FortiOS v6.2.16以上、v6.4.15以上、v7.0.14以上、v7.2.7以上、v7.4.3以上

FortiProxy v2.0.14以上 v7.0.15以上 v7.2.9以上 v7.4.3以上

4. 一時的なワークアラウンドについて

SSL VPN を無効にします(Web モードを無効にすることは有効な回避策ではありません)

URL :

<https://www.fortiguard.com/psirt/FG-IR-24-015>

以上