2023 年 7 月 12 日
株式会社ネットワールド

# FortiOS/FortiProxy - 詳細な検査を備えたプロキシ モード - スタックベースのバッファ 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 および FortiProxy のスタックベースのオーバーフローの脆弱性［CWE-124］により、リモート攻撃者は、SSL ディープ パケット インスペクションと並行してプロキシ モードを使用するプロキシ ポリシーまたはファイアウォール ポリシーに到達する、細工されたパケットを介して任意のコードまたはコマンドを実行する可能性があります。

CVE ID：
CVE-2023-33308

**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 ～ 7.2.3
FortiOS バージョン 7.0.0 ～ 7.0.10
FortiProxy バージョン 7.2.0 ～ 7.2.2
FortiProxy バージョン 7.0.0 ～ 7.0.9

影響を受けない製品:
FortiOS 6.4 すべてのバージョン
FortiOS 6.2 すべてのバージョン
FortiOS 6.0 すべてのバージョン
FortiProxy 2.x すべてのバージョン
FortiProxy 1.x すべてのバージョン

ワークアラウンド：
プロキシポリシーまたはプロキシモードのファイアウォール ポリシーによって使用される SSL 検査プロファイルでの HTTP/2 サポートを無効にします。

custom-deep-inspectionプロファイルの例:

```
config firewall ssl-ssh-profile
edit "custom-deep-inspection"
set supported-alpn http1-1
next
end
```

URL：
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection

該当するバージョンをご利用のお客様は以下のアップグレードをお願いします。

ソリューション：
FortiOS バージョン 7.2.4 以降にアップグレードしてください。
FortiOS バージョン 7.0.11 以降にアップグレードしてください。
FortiProxy バージョン 7.2.3 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。

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

以上