2024 年 3 月 13 日
株式会社ネットワールド

FortiOS および FortiProxy - キャプティブ ポータルの範囲外書き込みの脆弱性について

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頂きます。

CVE ID：
FG-IR-23-328

1. 対象製品について

【対象 OS】
FortiOS バージョン 7.4.0 ～ 7.4.1
FortiOS バージョン 7.2.0 ～ 7.2.5
FortiOS バージョン 7.0.0 ～ 7.0.12
FortiOS バージョン 6.4.0 ～ 6.4.14
FortiOS バージョン 6.2.0 ～ 6.2.15
FortiProxy バージョン 7.4.0
FortiProxy バージョン 7.2.0 ～ 7.2.6
FortiProxy バージョン 7.0.0 ～ 7.0.12
FortiProxy バージョン 2.0.0 ～ 2.0.13
FortiOS バージョン 6.x は影響を受けません。

2. 概要について
FortiOS および FortiProxy に境界外書き込みの脆弱性［CWE-787］およびスタックバッファオーバーフローの脆弱性 ［CWE-121]が内在し、悪意のある攻撃者がリモートからキャプティブポータル経由で特別に細工された 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。

対策済FOSバージョン
FortiOS バージョン 7.4.2 またはそれ以降
FortiOS バージョン 7.2.6 またはそれ以降
FortiOS バージョン 7.0.13 またはそれ以降

FortiOS バージョン 6.4.15 またはそれ以降
FortiOS バージョン 6.2.16 またはそれ以降
FortiProxy バージョン 7.4.1 またはそれ以降
FortiProxy バージョン 7.2.7 またはそれ以降
FortiProxy バージョン 7.0.13 またはそれ以降
FortiProxyバージョン 2.0.14 またはそれ以降

4. ワークアラウンド

フォーム認証以外のschemeを設定する。
（set method formで設定されている場合、以下の**method**に変更してください）

```
config authentication scheme
  edit scheme
    set method <method>
  next
end
```

<**method**>は以下の認証のいずれかでございます。

ntlm	NTLM authentication.
basic	Basic HTTP authentication.
digest	Digest HTTP authentication.
negotiate	Negotiate authentication.
fsso	Fortinet Single Sign-On (FSSO) authentication.
rsso	RADIUS Single Sign-On (RSSO) authentication.
ssh-publickey	Public key based SSH authentication.
cert	Client certificate authentication.
saml	SAML authentication

URL：最新の情報は、下記のリンク先についてご確認ください。
https://fortiguard.fortinet.com/psirt/FG-IR-23-328

以上