2024 年 2 月 16 日
株式会社ネットワールド

FortiOS – fgfmd のフォーマット文字列のバグについて

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：
CVE-2024-23113

1. 対象製品について

【対象 OS】
対象 FOS バージョン
FortiOS バージョン 7.4.0 - 7.4.2
FortiOS バージョン 7.2.0 - 7.2.6
FortiOS バージョン 7.0.0 - 7.0.13

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 fgfmd デーモンプロセスに脆弱性 [CWE-134] が内在し、リモートの攻撃者が、特別に細工された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す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 7.4.3 およびそれ以降
FortiOS バージョン 7.2.7 およびそれ以降
FortiOS バージョン 7.0.14 およびそれ以降

4. ワークアラウンド
各インターフェイスについて、 fgfm アクセスを削除します。たとえば、次のように変更します。

```
config system interface
edit "portX"
set allowaccess ping https ssh fgfm
next
end
```

to :

```
config system interface
edit "portX"
set allowaccess ping https ssh
next

end
```

これにより、FortiManager から FortiGate が検出されなくなることに注意してください。FortiGate からの接続は引き続き機能します。

特定の IP からの FGFM 接続のみを許可するローカルイン ポリシーは攻撃対象領域を減らしますが、この IP からの脆弱性の悪用を防ぐことはできないことにも注意してください。したがって、これは完全な回避策としてではなく、緩和策として使用する必要があります。

URL :
https://www.fortiguard.com/psirt/FG-IR-24-029

以上