2024 年 10 月 24 日
株式会社ネットワールド

FortiManager fgfmsd 認証欠如の脆弱性について

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：
FortiManager fgfmd デーモンの重大な機能脆弱性［CWE-306］に対する認証の欠如により、
認証されていないリモートの攻撃者が特別に細工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-2024-47575

影響：
許可されていないコードやコマンドを実行する

影響を受ける製品：
FortiManager 7.6.0
FortiManager 7.4.0 ～ 7.4.4
FortiManager 7.2.0 ～ 7.2.7
FortiManager 7.0.0 ～ 7.0.12
FortiManager 6.4.0 ～ 6.4.14
FortiManager 6.2.0 ～ 6.2.12
FortiManager Cloud 7.4.1 ～ 7.4.4
FortiManager Cloud 7.2.1 ～ 7.2.7
FortiManager Cloud 7.0.1 ～ 7.0.12
FortiManager Cloud 6.4 すべてのバージョン

対策：
FortiManager 7.6.1 またはそれ以上にアップグレードしてください。
FortiManager 7.4.5 またはそれ以上にアップグレードしてください。
FortiManager 7.2.8 またはそれ以上にアップグレードしてください。
FortiManager 7.0.13 またはそれ以上にアップグレードしてください。
FortiManager 6.4.15 またはそれ以上にアップグレードしてください。
FortiManager 6.2.13 またはそれ以上にアップグレードしてください。

FortiManager Cloud 7.4.5 またはそれ以上にアップグレードしてください。
FortiManager Cloud 7.2.8 またはそれ以上にアップグレードしてください。
FortiManager Cloud 7.0.13 またはそれ以上にアップグレードしてください。
FortiManager Cloud 6.4 上記、Fixバージョンへアップグレードしてください。

※FortiManager Cloud 7.6は影響なし

回避方法：
1- FortiManager 7.0.12 以上、7.2.5 以上、7.4.3 以上（7.6.0 は除く）の場合、
不明なデバイスの登録を防止します。

```
config system global
(global)# set fgfm-deny-unknown enable
(global)# end
```

2- あるいは、FortiManager 7.2.0 以降では、ローカルインポリシーを追加して、接続が許可される FortiGate の IP アドレスをホワイトリストに登録することもできます。

例：

```
config system local-in-policy
edit 1
set action accept
set dport 541
set src
next
edit 2
set dport 541
next
end
```

3- 7.2.2 以上、7.4.0 以上、7.6.0 以上では、問題を軽減するカスタム証明書を使用することもできます。

```
config system global
set fgfm-ca-cert
set fgfm-cert-exclusive enable
end
```

そして、その証明書を FortiGate にインストールします。この CA のみが有効になります。これは、攻撃者が代替チャネル経由でこの CA によって署名された証明書を取得できない場合に回避策として機能します。

侵害の兆候：
考えられる IoC は次のとおりです。
ログエントリ：
---
type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="device,...",msg="Unregistered device localhost add succeeded" device="localhost" adom="FortiManager" session_id=0 operation="Add device" performed_on="localhost" changes="Unregistered device localhost add succeeded"
---
type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,at,notice,level",user="System",userfrom="",msg="" adom="root" session_id=0 operation="Modify device" performed_on="localhost" changes="Edited device settings (SN FMG-VMTM23017412)"

IPアドレス：
45.32.41.202
104.238.141.143
158.247.199.37
45.32.63.2

シリアルナンバー：
FMG-VMTM23017412

ファイル：
/var/tmp/.tmのファイル
ファイル IoC は必ずしもすべてのケースで表示されるわけではないことに注意してください。

リスク：
実際に確認されているこの攻撃のアクションは、管理対象デバイスの IP、資格情報、および設定を含むさまざまなファイルを FortiManager からスクリプト経由で自動的に抽出するというものでした。

現時点では、これらの侵害された FortiManager システムにマルウェアやバックドアが低レベルのシステム インストールされたという報告は受けていません。
当社が知る限り、データベースが変更された兆候や、管理対象デバイスへの接続や変更があったという兆候は見られません。

Recovery(回復)：
FortiManager 設定のバックアップ ファイルには、OS またはシステム レベルのファイルの変更は含まれません。
これらのファイルはアーカイブに含まれていないためです。したがって、侵害されたシステムからバックアップを取り、それを新しいシステムまたは再初期化されたシステムに復元しても、このような低レベルの変更は引き継がれず、再導入されることはありません。

この方法を採用する場合は、データが改ざんされている可能性があることに注意してください。設定の正確性を確認するために、慎重に確認する必要があります。

以下の方法は、バックアップに含まれる管理対象デバイス (FortiGate など)が改ざんされておらず、その設定が信頼できることを前提としています。

FortiGateのイベント ログ アクティビティの検証は、特定された IoC の日付から開始して確認し、不正アクセスや設定変更があったかどうかを確認する必要があります。

FortiManagerデータベースからデータが流出している可能性があるため、すべての管理対象デバイスのパスワードやユーザーの機密データなどの認証情報を緊急に変更することをお勧めします。

VM インストールの場合、侵害された FortiManager のコピーをインターネットに接続されていない隔離されたネットワークに保存し、オフライン モードとクローズド ネットワーク モード操作(以下の設定を参照) で設定することで、回復が容易になります。
このシステムを使用して、並行してセットアップされる新しいシステムと比較できます。

```
config system admin setting
set offline_mode enable
end
config fmupdate publicnetwork
set status disabled
end
```

Recovery Methods(回復方法)：
オプション 1 - 推奨される回復アクション
この方法により、FortiManager の設定が改ざんされていないことが保証されます。
デバイスおよびポリシー パッケージ ADOM レベルでデータベースの再構築またはデバイス設定の再同期が必要になります。

・新しい FortiManager VM をインストールするか、ハードウェア モデルを再初期化してデバイスを追加/検出します。
・新しい FortiManager VM をインストールするか、ハードウェア モデルを再初期化して、IoC 検出前に取得したバックアップを復元します。

オプション2 - 代替回復アクション
この方法は、データベースの再構築や再同期を部分的に行うか、まったく行わずに、迅速なリカバリを実現します。
現在実行中のFortiManager設定の正確性を手動で確認する必要があります。

・新しい FortiManager VM をインストールするか、ハードウェア モデルを再初期化し、侵害された FortiManagerからコンポーネントまたは設定セクションを復元/コピーします。
・新しい FortiManager VM をインストールするか、ハードウェア モデルを再初期化し、侵害された FortiManager からバックアップを復元します。

データ構成と同期手順の詳細については、
https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-data-configuration-and/ta-p/351748 をご覧ください。

最新の情報は、下記のリンク先にてご確認ください。
https://www.fortiguard.com/psirt/FG-IR-24-423

以上