2022 年 10 月 11 日
株式会社ネットワールド

FortiOS/FortiProxy/FortiSwitchManager - 管理インターフェースでの認証バイパスについて

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、FortiProxy、および FortiSwitchManager の代替パスまたはチャネルの脆弱性
[CWE-288] を使用した認証バイパスにより、認証されていない攻撃者が、特別に細工された
HTTP または HTTPS リクエストを介して管理インターフェイスで操作を実行できる可能性
があります。

CVE ID：
CVE-2022-40684

影響：
許可されていないコードまたはコマンドを実行する

Exploitation Status:
フォーティネットは、この脆弱性が悪用された例を認識しており、デバイスのログにある
次の侵害の兆候に対してシステムをすぐに検証することをお勧めします。

user="Local_Process_Access"

サポートが必要な場合は、カスタマー サポートにお問い合わせください。

回避策:
FortiOS:
HTTP/HTTPS 管理インターフェースを無効にする
または、
管理インターフェースに到達できる IP アドレスを制限します。

```
config firewall address
edit "my_allowed_addresses"
set subnet <MY IP> <MY SUBNET>
end
```

次に、アドレス グループを作成します。

```
config firewall addrgrp
edit "MGMT_IPs"
set member "my_allowed_addresses"
end
```

ポリシーでローカルを作成して、管理インターフェイス（ここではポート 1）の事前定義されたグループへのアクセスのみを制限します。

```
config firewall local-in-policy
edit 1
set intf port1
set srcaddr "MGMT_IPs"
set dstaddr "all"
set action accept
set service HTTPS HTTP
set schedule "always"
set status enable
next
edit 2
set intf "all"
set srcaddr "all"
set dstaddr "all"
set action deny
set service HTTPS HTTP
set schedule "always"
set status enable
end
```

デフォルト以外のポートを使用する場合は、GUI 管理アクセス用の適切なサービスオブジェクトを作成します。

```
config firewall service custom
edit GUI_HTTPS
set tcp-portrange <admin-sport>
next
edit GUI_HTTP
set tcp-portrange <admin-port>
end
```

以下の local-in ポリシー 1 および 2 では、「HTTPS HTTP」の代わりにこれらのオブジェクトを使用します。
サポートが必要な場合は、カスタマー サポートにお問い合わせください。

FortiProxy:
HTTP/HTTPS 管理インターフェースを無効にする
または、
管理インターフェース（ここでは port1）に到達できる IP アドレスを制限します。

```
config system interface
edit port1
set dedicated-to management
set trust-ip-1 <MY IP> <MY SUBNET>
end
```

サポートが必要な場合は、カスタマー サポートにお問い合わせください。

影響を受ける製品：
FortiOS バージョン 7.2.0 ～ 7.2.1
FortiOS バージョン 7.0.0 ～ 7.0.6
FortiProxy バージョン 7.2.0
FortiProxy バージョン 7.0.0 ～ 7.0.6
FortiSwitchManager バージョン 7.2.0
FortiSwitchManager バージョン 7.0.0

ソリューション：
FortiOS バージョン 7.2.2 以降にアップグレードしてください。
FortiOS バージョン 7.0.7 以降にアップグレードしてください。
FortiProxy バージョン 7.2.1 以降にアップグレードしてください。
FortiProxy バージョン 7.0.7 以降にアップグレードしてください。
FortiSwitchManager バージョン 7.2.1 以降にアップグレードしてください。

URL：
https://www.fortiguard.com/psirt/FG-IR-22-377

以上