2023 年 3 月 8 日
株式会社ネットワールド

FortiOS / FortiProxy - 管理インターフェイスのヒープバッファアンダーフローについて

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 管理インターフェイスのバッファアンダーライト（「バッファアンダーフロー」）の脆弱性により、リモートの認証されていない攻撃者が、特別に細工されたリクエストを介して、デバイスで任意のコードを実行したり、GUI で DoS を実行したりできる可能性があります。

CVE ID：
CVE-2023-25610

影響：
サービス拒否

Exploitation Status:
フォーティネットは、この脆弱性が実際に悪用された事例を認識していません。
当社は製品のセキュリティを継続的に見直し、テストしており、この脆弱性はそのフレーム内で内部的に発見されました。

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 ～ 7.0.9
FortiOS バージョン 6.4.0 ～ 6.4.11
FortiOS バージョン 6.2.0 ～ 6.2.12
FortiOS 6.0 すべてのバージョン
FortiProxy バージョン 7.2.0 ～ 7.2.2
FortiProxyバージョン 7.0.0 から 7.0.8
FortiProxy バージョン 2.0.0 から 2.0.11
FortiProxy 1.2 すべてのバージョン
FortiProxy 1.1 すべてのバージョン

ソリューション：
FortiOS バージョン 7.4.0 以降にアップグレードしてください。
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 7.0.10 以降にアップグレードしてください 。
FortiOS バージョン 6.4.12 以降にアップグレードしてください 。
FortiOS バージョン 6.2.13 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 7.0.9 以降にアップグレードしてください 。
FortiProxy バージョン 2.0.12 以降にアップグレードしてください。
FortiOS-6K7K バージョン 7.0.10 以降にアップグレードしてください。
FortiOS-6K7K バージョン 6.4.12 以降にアップグレードしてください。
FortiOS-6K7K バージョン 6.2.13 以降にアップグレードしてください。

なお、影響のあるFortiOS バージョンを利用している場合でも、以下にリストされている
ハードウェアデバイスは、問題の DoS のみの影響を受け、任意のコードの実行による
影響を受けません。（リストされていないデバイスは両方に対して脆弱です):

FortiGateRugged-100C
FortiGate-100D
FortiGate-200C
FortiGate-200D
FortiGate-300C
FortiGate-3600A
FortiGate-5001FA2
FortiGate-5002FB2
FortiGate-60D
FortiGate-620B
FortiGate-621B
FortiGate-60D-POE
FortiWiFi-60D
FortiWiFi-60D-POE
FortiGate-300C-Gen2
FortiGate-300C-DC-Gen2
FortiGate-300C-LENC-Gen2
FortiWiFi-60D-3G4G-VZW
FortiGate-60DH
FortiWiFi-60DH
FortiGateRugged-60D
FortiGate-VM01-Hyper-V
FortiGate-VM01-KVM
FortiWiFi-60D-I

FortiGate-60D-Gen2

FortiWiFi-60D-J

FortiGate-60D-3G4G-VZW

FortiWifi-60D-Gen2

FortiWifi-60D-Gen2-J

FortiWiFi-60D-T

FortiGateRugged-90D

FortiWifi-60D-Gen2-U

FortiGate-50E

FortiWiFi-50E

FortiGate-51E

FortiWiFi-51E

FortiWiFi-50E-2R

FortiGate-52E

FortiGate-40F

FortiWiFi-40F

FortiGate-40F-3G4G

FortiWiFi-40F-3G4G

FortiGate-40F-3G4G-NA

FortiGate-40F-3G4G-EA

FortiGate-40F-3G4G-JP

FortiWiFi-40F-3G4G-NA

FortiWiFi-40F-3G4G-EA

FortiWiFi-40F-3G4G-JP

FortiGate-40F-Gen2

FortiWiFi-40F-Gen2

回避策:

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
```

Local-in-Policy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に制限します。

```
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 "any"
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している場合は、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
```

HA 管理インターフェイスを使用している場合、local-in-Policyを少し異なる方法で設定する必要があります。以下をご参考ください。

URL：
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005

URL：
https://www.fortiguard.com/psirt/FG-IR-23-001

以上