2023 年 3 月 29 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiOS 管理インターフェース(GUI)のバッファアンダーフローの脆弱性(CVE-2023-25610)について(第五報)

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiOS 管理インターフェース(GUI)のバッファアンダーフローの脆弱性(CVE-2023-25610)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様は、対策済み OS へのバージョンアップについて、ご検討をお願いいたします。

※太字箇所が、第五報での追記もしくは更新箇所となっています。

敬具

記

1. 事象の概要

FortiOS において、管理インターフェース(GUI)にバッファアンダーフローの脆弱性があり、外部からの認証されていない攻撃者に、悪意を持って細工した HTTP リクエストを介して、FortiGate 上で任意のコードが実行される可能性があります。また、プロセスが利用している動的メモリ空間を操作して、プロセスクラッシュを連続して発生させることで DoS 攻撃となる可能性があります。

Fortinet 社からは、現時点で本脆弱性を悪用した攻撃を検知していないとのアナウンスがされています。

詳細、最新の情報については Fortinet 社から発表されています以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

FortiOS / FortiProxy - Heap buffer underflow in administrative interface
<https://www.fortiguard.com/psirt/FG-IR-23-001>

2. 該当製品と対策バージョン

脆弱性の影響を受けるバージョン、及び対策バージョンは以下の通りです。

影響を受けるバージョンをご利用中の場合は、対策済み OS へのバージョンアップをお願いいたします。

項	メジャーバージョン	影響を受ける バージョン	対策 バージョン	備考
1	FortiOS 7.2 系	7.2.0 ～ 7.2.3	7.2.4 以降	
2	FortiOS 7.0 系	7.0.0 ～ 7.0.9	7.0.10 以降	
3	FortiOS 6.4 系	6.4.0 ～ 6.4.11	6.4.12 以降	
4	FortiOS 6.2 系	6.2.0 ～ 6.2.12	6.2.13 以降	
5	FortiOS 6.0 系	6.0.0 ～ 6.0.16	**6.0.17 以降 (予定)**	6.0 系 OS はメーカーサポート終了済(EOS 済み)
6	**FortiOS 5.x 系**	**全ての バージョン**	**現時点で なし**	**5.x 系 OS はメーカーサポート終了済(EOS 済み)**

項	メジャーバージョン	影響を受ける バージョン	対策 バージョン	備考
7	FortiOS(6000 シリーズ) 7.0 系	**7.0.5**	7.0.10(※1) 以降	
8	FortiOS(6000 シリーズ) 6.4 系	**6.4.2, 6.4.6, 6.4.8, 6.4.10**	6.4.12(※2) 以降	
9	FortiOS(6000 シリーズ) 6.2 系	**6.2.4, 6.2.6, 6.2.7, 6.2.9～6.2.12**	6.2.13(※3) 以降	
10	**FortiOS(6000 シリーズ) 6.0 系**	**全ての バージョン**	**現時点で なし**	**6000 シリーズの 6.0 系 OS は弊社未リリース**

※1 2023 年 3 月 14 日に弊社からリリース済です。

※2 2023 年 3 月 15 日に弊社からリリース済です。

※3 2023 年 3 月 10 日に弊社からリリース済です。

3. 回避策

脆弱性の回避策は以下の通りです。なお、回避策 2 によりアクセス元の IP アドレスを制限した後も、該当 IP アドレスからのアクセスには脆弱性が残るため、早急に対策バージョンへのアップグレードの検討をお願いいたします。

回避策 1

FortiGate の GUI への HTTP/HTTPS によるアクセスを無効化することにより、本脆弱性が回避可能です。なお、本回避策を適用すると、GUI を利用した管理アクセスが出来なくなります。

回避策 2

local-in-policy により、FortiGate の管理インターフェース(GUI)へのアクセス元の IP アドレスを制限することで、制限した IP アドレス以外からの脆弱性を回避可能です。

local-in-policy による管理インターフェースへのアクセス制限の設定例を以下に示します。

(1)GUI へのアクセス許可するアドレス
オブジェクトを作成します

```
----------------------------------------------
config firewall address
 edit <アドレスオブジェクト名>
  set subnet <IP アドレス> <サブネット>(※1)
 next
end
----------------------------------------------
```

(2) (1)で作成したアドレスオブジェクトの
アドレスグループを作成します

```
----------------------------------------------
config firewall addrgrp
 edit <アドレスグループ名>
  set member <アドレスオブジェクト名>
 next
end
----------------------------------------------
```

(3) 管理インターフェース(GUI)に対する
local-in-policy を作成します

```
----------------------------------------------
config firewall local-in-policy
 edit 1(※2)
  set intf <管理インターフェース>(※3)
  set srcaddr <アドレスグループ名>
  set dstaddr "all"
  set action accept
  set service HTTPS HTTP (※4)
  set schedule "always"
  set status enable
 next
 edit 2(※2)
  set intf "any"
  set srcaddr "all"
  set dstaddr "all"
  set action deny
  set service HTTPS HTTP (※4)
  set schedule "always"
  set status enable
 next
end
----------------------------------------------
```

※1 アクセスを許可する IP アドレス、サブネットマスクを指定してください。
※2 設定を 2 つ作成して、特定のアドレスグループからの管理インターフェース(GUI)へのアクセスのみを許可して、それ以外の HTTPS, HTTP のアクセスを禁止します。
※3 HA reserved management interface を利用している場合は、以下のページを参照して設定してください。
Technical Tip: How to configure a local-in policy on a HA reserved management interface
<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005>
※4 管理インターフェースへのアクセスにデフォルトポート(HTTPS, HTTP)以外を利用している場合は、利用しているポートをサービスオブジェクトとして登録して、そのサービスを指定してください。

4. OS ファイルの入手方法

バージョンアップは、対象機器がインターネットに接続している場合は、GUI で OS のダウンロード、及びバージョンアップを行うことができます。

OS ファイルがご入用の場合は、弊社サポートからご提供しております。対象機器のシリアル番号（S/N）と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上