2025 年 01 月 15 日
株式会社ネットワールド

Node.js Websocket モジュール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 および FortiProxy に影響する代替パスまたはチャネルを使用した認証バイパス
の脆弱性［CWE-288］により、リモートの攻撃者が Node.js Websocket モジュールへの細工
されたリクエストを介してスーパー管理者権限を取得できる可能性があります。

CVE ID：
CVE-2024-55591

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：
FortiOS 7.0.0 ～ 7.0.16
FortiProxy 7.2.0 ～ 7.2.12
FortiProxy 7.0.0 ～ 7.0.19

※以下のバージョンは影響はございません。
FortiOS 7.6
FortiOS 7.4
FortiOS 7.2
FortiOS 6.4
FortiProxy 7.6
FortiProxy 7.4
FortiProxy 2.0

対策：
FortiOS 7.0.17以上にアップグレードしてください。
FortiProxy 7.2.13以上にアップグレードしてください。
FortiProxy 7.0.20以上にアップグレードしてください。

IoC
次のログ エントリは IOC の可能性があります。
ランダム スクリプトと dstip を含む次のログイン アクティビティ ログ:

type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1733486785" user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin logged in successfully from jsconsole"

ランダムに生成されたユーザー名とソース IP を含む次の管理者作成ログ:

type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="admin" ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin" cfgobj="vOcep" cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin vOcep"

上記のログでは、攻撃者が主に使用している IP アドレスは次のとおりでした:
1.1.1.1
127.0.0.1
2.2.2.2
8.8.8.8
8.8.4.4

私たちが観察したケースで脅威アクター（TA）が実行した操作は、以下の一部またはすべてでした。
- ランダムなユーザー名でデバイス上に管理者アカウントを作成する
- ランダムなユーザー名でデバイス上にローカル ユーザー アカウントを作成する
- ユーザー グループを作成するか、上記のローカル ユーザーを既存の sslvpn ユーザー グループに追加する
- その他の設定（ファイアウォール ポリシー、ファイアウォール アドレスなど）を追加/変更する
- 上記の追加したローカル ユーザーで sslvpn にログインして、内部ネットワークへのトンネルを取得する。

TA によって作成された管理者またはローカル ユーザーはランダムに生成されます。例:
Gujhmk
Ed8x4k
G0xgey
Pvnw81
Alg7c4
Ypda8a
Kmi8p4
1a2n6t
8ah1t6
M4ix9f
... など...

さらに、TA は次の IP アドレスを使用していることが確認されています。

45.55.158.47［最も使用されているIPアドレス］
87.249.138.47
155.133.4.175
37.19.196.65
149.22.94.37

回避策：
HTTP/HTTPS管理インターフェースを無効にする
または
Local in Policyを使用して管理インターフェイスにアクセスできる IP アドレスを制限します。

ファイアウォールアドレスの設定
config firewall address
edit "my_allowed_addresses"
set 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

管理インターフェイス（ここでは port1）上の定義済みグループのみにアクセスを制限するLocal in Policyを作成します。

```
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 443
next

edit GUI_HTTP
set tcp-portrange 80
end
```

以下のLocal in Policy 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。
すべての GUI ユーザーが trusthost 機能を使用して設定されている場合にのみ、
trusthost 機能は上記のLocal in Policyと同じ効果を発揮することに注意してください。
したがって、上記の Local in Policyが推奨される回避策です。

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

以上