2021 年 6 月 24 日
株式会社ネットワールド

FortiManager での認証されていないリモートコードの実行について

このたび Fortinet 社が提供する FortiManager 製品にて以下情報が公開されましたので、
以下の通りご報告させて頂きます。

1. 説明：
   FortiManager デーモンの脆弱性により、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ターゲットデバイスに送信することにより、
   root として不正なコードを実行する可能性があります。

   重大度：重大（9.6）

   影響：リモートコード実行

   影響の詳細：この脆弱性により、リモートの攻撃者がrootとして任意のコードを実行できる可能性があります。

   このCSBは、この脆弱性を顧客に早期に通知するために使用されます。FortiGuardパブリックアドバイザリは後日公開されます。

影響を受ける可能性のある製品：
FortiManager

影響を受ける可能性のあるOS：
FortiManagerバージョン5.6.10以下、6.0.10以下、6.2.7以下、6.4.5以下、7.0.0

解決：
FortiManagerを次のバージョンにアップグレードしてください。
5.6.11以降、6.0.11以降、6.2.8以降、6.4.6以降、7.0.1以降。

回避策：
影響を受けるサービスをFortiManagerで無効にすることはできません。
悪用を防ぐために、ネットワークレベルでFortiManagerデバイスにアクセスするための入力トラフィックのフィルタリング（つまり、信頼できるIPアドレスのみの許可）が必要です。

FortiManagerが有効なIPSサブスクリプションを持つFortiGateの背後にある場合、
次のIPSシグネチャを使用して、IPS定義18.100で利用可能なこの問題を軽減できます。

https://www.fortiguard.com/encyclopedia/ips/50483

以上