【重要】FFRI AMC における任意のコマンド実行可能な脆弱性について

2024 年 7 月 29 日
株式会社FFRI セキュリティ

平素より弊社製品をご利用頂きまして誠にありがとうございます。

FFRI セキュリティが提供する FFRI AMC において、『通知プログラム設定』を有効にしていて、『実行プログラム』に拡張子がバッチファイル（.bat）またはコマンドファイル（.cmd）を設定している環境で条件を満たすと、クライアント側から任意のコマンドを実行することが可能となる脆弱性が確認されました。
本脆弱性の対策として、修正モジュールの提供を行っております。
お手数をおかけいたしますが、ご適用いただきますようお願いいたします。

なお、本脆弱性は弊社自身で発見しており、現時点でこの脆弱性に関連する報告やお問合せは受けておらず、実際の攻撃も認識していません。

共通脆弱性評価システム（CVSS） 3.1 でのスコアは『8.1』となります。

影響を受ける製品の詳細は以下のとおりです。

ベンダー	製品名	バージョン	ベンダーのサイト
株式会社 FFRI セキュリティ	FFRI AMC	3.4.0～3.4.6 3.5.0～3.5.3	https://www.ffri.jp/security-info/index.htm
日本電気 株式会社	ActSecure χ	3.4.0～3.4.6 3.5.0～3.5.3	https://www.support.nec.co.jp/View.aspx?id=3140109694
Sky株式会社	EDR プラスパック	（同梱の FFRI AMC のバージョンに依存）	https://www.skyseaclientview.net/news/240729_01/

※上記以外のバージョンは影響を受けません。また、FFRI yarai Cloud は本脆弱性の影響を受けておりません。

※上記の製品・上記のバージョンをご利用の場合でも、『通知プログラム設定』を有効にしていない環境、または有効でも『実行プログラム』に拡張子がバッチファイル（.bat）またはコマンドファイル（.cmd）

を設定していない環境、または後述の『[暫定的な対策を実施する] - 通知プログラム設定を無効にする』設定を行っていれば影響を受けません。

・想定される影響

FFRI yarai から FFRI AMC に対して送られる通信を、攻撃者が偽装・改ざんすることにより、FFRI AMC の脆弱性を悪用して、サーバー側で任意のコマンドを実行することができます。

『通知プログラム設定』を使っていない場合、影響はありません。

『通知プログラム設定』を使っていても、「実行ファイル名」の設定で拡張子が『.bat』『.cmd』ではない場合、影響はありません。

上記に該当する場合でも、設定によっては影響を受けない場合もあります。

・対策

[アップデートする]

・お使いの製品が『FFRI AMC』の場合（月額版やマネージドサービスは除く） / 『EDR プラスパック』の場合

FFRI AMC は、弊社カスタマーサイトから最新版を取得しアップデートしてください。
3.6.1 が最新版となります。

カスタマーサイト（https://yarai.fourteenforty.jp/clients/）

※ログインにはユーザー名/パスワードが必要です

※FFRI yarai Cloud は本脆弱性の影響を受けていないため、対策は必要ありません

・上記以外の製品の場合

提供元のサポート窓口やサポートサイトにご確認ください。

[暫定的な回避策を実施する]
以下のいずれかの回避策を実施することで、本脆弱性の影響を受けなくなります。

＊ 通知プログラム設定を無効にする

上記の設定を行うと、通知プログラム設定による通知機能が利用できなくなります。

＊ 通知プログラム設定の『実行ファイル名』に指定するプログラムに、拡張子が『.bat』『.cmd』ではない別のファイルを設定する

[軽減策を実施する]
以下のような軽減策を実施することで、本脆弱性の影響を受ける可能性を軽減できます。

＊ FFRI AMC にアクセス可能な端末を制限する

＊ 信頼できないネットワークから FFRI AMC へのアクセスを制限する

以上