【重要】FFRI yarai および FFRI yarai Home and Business Edition における例外条件の不適切な処理の脆弱性について

2023 年 8 月 7 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 yarai および FFRI yarai Home and Business Edition において、

Windows Defender 連携機能を有効にしている環境で、特定のファイルを Microsoft Defender（旧名称・Windows Defender）が脅威として検知した際、FFRI yarai 側で情報を適切に処理できないため、FFRI yarai の監視機能（Scan Engine Service）が最大で 15 分間停止するサービス運用妨害（DoS）状態となる不具合が確認されました。
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、外部からリモート実行されるような問題ではありません。また、現時点で、この脆弱性に関連する影響を受ける製品に対する報告を受けておらず、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『4.3』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 yarai	3.4.0～3.4.6 3.5.0	https://www.ffri.jp/security-info/index.htm
株式会社 FFRI セキュリティ	FFRI yarai Home and Business Edition	1.4.0	https://www.ffri.jp/security-info/index.htm
株式会社 ソリトンシステムズ	InfoTrace Mark II マルウェア防御（Mark II Zerona）	V3.0.1 ～ V3.2.2	https://www.soliton.co.jp/support/zerona_notice_2023.html
株式会社 ソリトンシステムズ	Zerona / Zerona PLUS マルウェア対策	V3.2.32～ V3.2.36	https://www.soliton.co.jp/support/zerona_notice_2023.html

日本電気株式会社	ActSecure χ	3.4.0～3.4.6 3.5.0	https://www.support.nec.co.jp/View.aspx?id=3140109240
ソースネクスト株式会社	二重の安心 Powered by FFRI yarai	1.4.1	https://www.sourcenext.com/support/i/2023/230718_01
Sky株式会社	EDR プラスパック	（同梱の FFRI yarai のバージョンに依存）	https://www.skyseaclientview.net/news/230807_01/
Sky株式会社	EDR プラスパック Cloud	（同梱の FFRI yarai のバージョンに依存）	https://www.skyseaclientview.net/news/230807_01/

※上記以外のバージョンは影響を受けません

※上記の製品・上記のバージョンをご利用の場合でも Microsoft Defender 自体を無効化している環境、または後述の『[暫定的な対策を実施する] - Windows Defender 連携機能を無効にする』にあ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

特定のファイルを Microsoft Defender が脅威として検知した際、その情報によっては FFRI yarai / FFRI yarai Home and Business の Windows Defender 連携機能が適切に処理できないため、以降のファイルのスキャンなどが一定期間行われなくなる可能性があります。Microsoft Defender による検知時のみ発生するため、定義ファイルの更新といった他の挙動では発生しません。

また本脆弱性は FFRI yarai / FFRI yarai Home and Business にのみ影響があり、本脆弱性を使って他のアプリケーションに影響を及ぼすことはありません。同様に Microsoft Defender の動作には影響はありません。

・対策

[アップデートする]

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

FFRI yarai は、弊社カスタマーサイトから最新版を取得していただいてアップデートしていただくか、
3.5.0 の場合はクライアント側コンソールからの更新を行ってください。
3.4.0～3.4.6 の場合は、3.4.7 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。

・お使いの製品が『FFRI yarai cloud』 / 『EDR プラスパック Cloud』の場合

管理コンソールからのアップデートを実施してください。

3.5.0 の場合はクライアント側コンソールからアップデートも可能です。
3.4.0～3.4.6 の場合はクライアント側コンソールから 3.4.7 へのアップデートはできません。

・お使いの製品が『FFRI yarai Home and Business Edition』 / 『二重の安心』の場合

クライアントのメインウインドウの「ステータス」画面から「アップデート」を行ってください。

・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。

[暫定的な対策を実施する]

＊ Windows Defender 連携機能を無効にする

下記の設定を行うと、Microsoft Defender の脅威の検出イベントが記録されなくなります。
（この設定は Microsoft Defender の動作を無効化するものではありません）

・お使いの製品が『FFRI yarai』 / 『ActSecure χ』の場合

【管理されたクライアントの場合】

FFRI AMC のポリシー配布機能で「AMC および yarai による監視対象イベント」の「脅威の検出イベント(正常)」 「脅威の検出イベント(異常)」のチェックを外して、ポリシーを配布する。

※「AMC および yarai による監視対象イベント」で全てのチェックを外した場合は「全ての情報を収集しない」にチェックを入れてください。チェックを入れないとポリシーを作成することができません。

【独立したクライアントの場合】

レジストリキーの[HKEY_LOCAL_MACHINE¥SOFTWARE¥FFR¥yarai] (32bit OS の場合)
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥FFR¥yarai] (64bit OS の場合)、
レジストリ値"DefenderEventType"が存在し、"DefenderEventType"の制御フラグ 0x01 と 0x08 が 0 になるように設定する。

詳細は FFRI yarai のユーザーマニュアル『Windows Defender 連携のイベントログの設定』をご確認ください。

・お使いの製品が『FFRI yarai Home and Business Edition』 / 『二重の安心 Powered by FFRI yarai』の場合

・レジストリキーの[HKEY_LOCAL_MACHINE¥SOFTWARE¥FFRI¥yarai] (32bit OS の場合)
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥FFRI¥yarai] (64bit OS の場合)、
REG_DWORD 型のレジストリ値"DisableDefender"を作成し、0x01 を設定する。

・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。

※文中の表記で、『Windows Defender(連携機能)』と『Microsoft Defender』が混在しております。『Microsoft Defender』は現在の名称、『Windows Defender』は旧来の名称となりますので、同一のものとなります。

弊社製品では旧来の名称を採用して機能の名称としているため、本資料でも弊社製品の機能名をご説明している箇所では『Windows Defender 連携機能』と記載いたしました。

以上