MELSOFT iQ AppPortal における複数の脆弱性

公開日 2022 年 5 月 12 日
三菱電機株式会社

■概要

三菱電機が提供する MELSOFT iQ AppPortal は、サーバソフトウェア VisualSVN Server を搭載しています。VisualSVN Server が使用している OSS(オープンソースソフトウェア)に、複数の脆弱性が存在することが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合、当該製品の情報漏えい又は情報改ざんが発生したり、当該製品がサービスの停止(DoS)状態に陥ったり、悪意のあるプログラムが実行される等の可能性があります。

これらの脆弱性の影響を受ける MELSOFT iQ AppPortal のバージョンを以下に示しますので、該当製品については対策方法に記載の内容を実施してください。

■CVSS スコア

・CVE-2020-13938 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H 基本値:5.5
・CVE-2021-26691 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
・CVE-2021-34798 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
・CVE-2021-3711 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
・CVE-2021-44790 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
・CVE-2022-22720 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
・CVE-2022-23943 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
・CVE-2022-0778 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5

■該当製品の確認方法

影響を受ける製品は以下のとおりです。

製品	形名	バージョン
MELSOFT iQ AppPortal	SW1DND-IQAPL-M	1.00A～1.26C

使用しているバージョン番号の確認方法は以下の通りです。

1. MELSOFT iQ AppPortal を起動し、「ヘルプ」メニューから「バージョン情報」を選択します。
2. 現れたウィンドウの下記の部分が、起動している MELSOFT iQ AppPortal のバージョン番号です。(図 1 参照)

図 1：MELSOFT iQ AppPortal バージョン情報画面

■脆弱性の説明

MELSOFT iQ AppPortal に搭載されているサーバソフトウェアである VisualSVN Server が使用している OSS(オープンソースソフトウェア)には、以下の脆弱性があります。

以下に示す脆弱性により、サービス停止(DoS)状態に陥る可能性があります。

・CVE-2020-13938: 認証の欠如(CWE-862)
・CVE-2021-34798: NULL ポインタデリファレンス(CWE-476)
・CVE-2022-0778: 無限ループ(CWE-835)

以下に示す脆弱性により、情報が改ざんされたり、サービス停止(DoS)状態に陥ったり、悪意のあるプログラムが実行される

等の可能性があります。
・CVE-2021-26691: 境界外書き込み(CWE-787)
・CVE-2021-3711: 古典的バッファオーバーフロー(CWE-120)
・CVE-2021-44790: 境界外書き込み(CWE-787)
・CVE-2022-23943: 境界外書き込み(CWE-787)

以下に示す脆弱性により、情報が漏えいしたり、情報が改ざんされたり、認証を回避される等の可能性があります。
・CVE-2022-22720: HTTP リクエストスマグリング(CWE-444)

■脆弱性がもたらす脅威
上記の脆弱性を悪意のある攻撃者に悪用されることにより、当該製品の情報漏えい又は情報の改ざんが発生したり、当該製品がサービス停止(DoS)状態に陥ったり、悪意のあるプログラムが実行される等の可能性があります。

■対策方法
以下サイトよりバージョン 1.29F 以降をダウンロードしたうえで、アップデートしてください。

https://www.mitsubishielectric.co.jp/fa/download/index.html

<アップデート方法>
1. ダウンロードしたファイル(zip 形式)を解凍します。
2. 解凍されたフォルダの中の「setup.exe」を実行してインストールを行ってください。

■回避策
すぐに製品をアップデートできないお客様に対して、これらの脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

(1) 当該製品を使用するパソコンのネットワークへの接続を最小限に抑え、信頼できるネットワークやホストからのみアクセスできるようにしてください。
(2) 当該製品を使用するユーザーの権限を必要最小限にしてください。
(3) 当該製品を使用するパソコンにウイルス対策ソフトを搭載してください。
(4) 当該製品のオペレーティングマニュアルに記載の「安全上のご注意」に従ってください。

■お客様からのお問い合わせ先
製品をご購入いただいた弊社の支社、代理店にご相談ください。

<お問い合わせ | 三菱電機 FA>
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html