MELSOFT iQ AppPortal における HTTP リクエストスマグリングの脆弱性と IP アドレスによる認証回避の脆弱性

公開日 2023 年 2 月 21 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。ユーザーが VisualSVN Server の設定にて mod_proxy や mod_proxy_ajp を有効化した場合に、VisualSVN Server が使用している Apache HTTP Server において、HTTP リクエストスマグリングの脆弱性(CVE-2022-26377)と IP アドレスによる認証を回避される脆弱性(CVE-2022-31813)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、認証を回避される、情報が漏えいする、サービス停止(DoS)状態に陥るなど、未確認の影響を受けたり、IP アドレスによる認証を回避される可能性があります。

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 [1]

・CVE-2022-26377 :CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:7.5
・CVE-2022-31813 :CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:9.8

■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～1.29F

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)

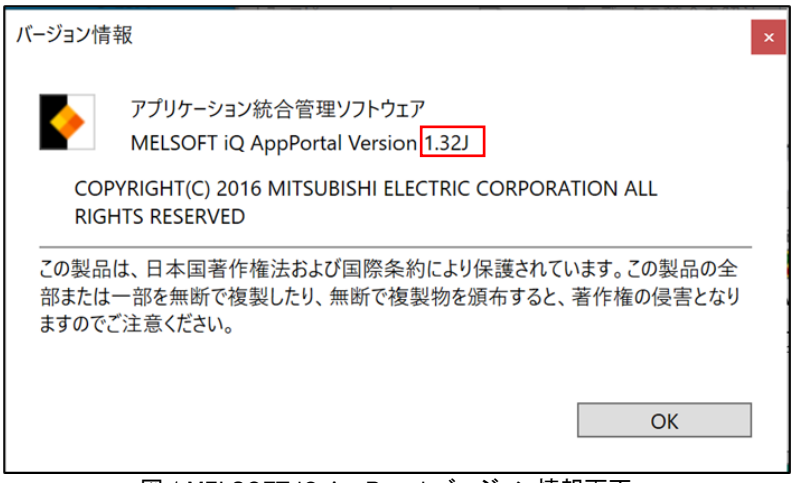

図 1.MELSOFT iQ AppPortal バージョン情報画面

■脆弱性の説明

ユーザーが VisualSVN Server の設定にて mod_proxy や mod_proxy_ajp を有効化した場合に、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 Apache HTTP Server には、HTTP リクエストスマグリングの脆弱性(CVE-2022-26377)と IP アドレスによる認証回避の脆弱性(CVE-2022-31813)の脆弱性があります。

以下に示す問題により、認証を回避される、情報が漏えいする、サービス停止(DoS)状態に陥るなど、未確認の影響を受ける可能性があります。

・CVE-2022-26377:HTTP リクエストスマグリング(CWE-444)[2]

以下に示す問題により、IP アドレスによる認証を回避される可能性があります。

・CVE-2022-31813:データの信頼性についての不十分な検証(CWE-345)[3]

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/444.html
3 https://cwe.mitre.org/data/definitions/345.html

■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、当該製品の認証を回避される、情報が漏えいする、サービス停止(DoS)状態に陥るなど、未確認の影響を受けたり、IP アドレスによる認証を回避される可能性があります。

■対策方法

以下サイトよりバージョン 1.32J 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。

■軽減策・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回避策または軽減策を講じることを推奨します。

〈回避策〉

(1) VisualSVN Server の設定にて、可能であれば mod_proxy や mod_proxy_ajp を無効化してください。

〈軽減策〉

(1) 当該製品をインストールしたパソコンをインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。
(2) 当該製品を使用するパソコンを LAN 内で使用し、かつファイアウォール等を使用して、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。
(3) 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。
(4) 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。

■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