Edgecross 基本ソフトウェア Windows 版における
複数の悪意のあるプログラムが実行される脆弱性

公開日 2024 年 11 月 21 日
最終更新日 2024 年 11 月 21 日
一般社団法人 Edgecross コンソーシアム

■概要

Edgecross 基本ソフトウェア Windows 版のバージョン 1.00 以降に複数の悪意のあるプログラムが実行される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に、悪意のあるプログラムが実行され、情報を取得されたり、情報を改ざん・破壊・削除されたり、対象をサービス停止(DoS)状態にされる等の可能性があります。

脆弱性の影響を受ける Edgecross 基本ソフトウェア Windows 版のバージョンを以下に示しますので、当該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-2024-4229 CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H 基本値:7.8
CVE-2024-4230 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基本値:7.8

■該当製品の確認方法

影響を受ける製品は以下の製品です。

・CVE-2024-4229

製品のインストール時に、管理者権限を持ったユーザのみに変更権限が与えられたフォルダ以外のフォルダを指定してインストールを行った場合にのみ、脆弱性の影響を受けます。

製品	型名	バージョン
Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W	1.00 以降
開発者用 Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W-D	1.00 以降

・CVE-2024-4230

製品	型名	バージョン
Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W	1.00 以降
開発者用 Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W-D	1.00 以降

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. Edgecross 基本ソフトウェア Windows 版リアルタイムフローデザイナを起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している Edgecross 基本ソフトウェア Windows 版のバージョン番号です。（図 1 参照）

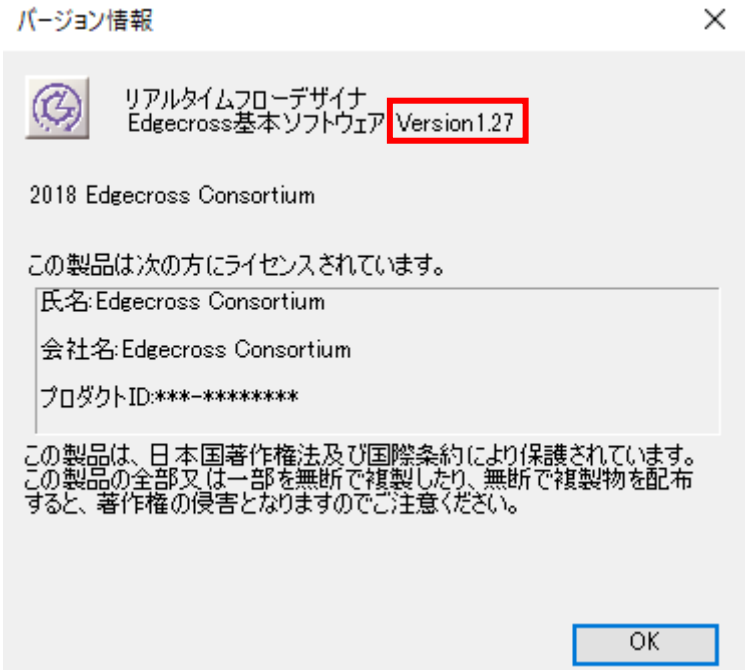

図 1:Edgecross 基本ソフトウェア Windows 版　バージョン情報画面(リアルタイムフローデザイナ)

■脆弱性の説明

以下に示す問題により、当該製品において悪意のあるプログラムが実行される可能性があります。

・CVE-2024-4229:　　不適切なデフォルトパーミッション(CWE-276)
・CVE-2024-4230:　　ファイル名やパス名の外部制御(CWE-73)

■脆弱性がもたらす脅威

これらの脆弱性を悪意のある攻撃者に悪用された場合に、悪意のあるプログラムが実行され、情報を取得される、情報を改ざん・破壊・削除される、サービス停止(DoS)状態にされる等の可能性があります。

■対策方法

回避策にて対応をお願いいたします。

■回避策

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、以下に示す回避策を講じることを推奨します。

CVE-2024-4229

・当該製品をデフォルトのインストールフォルダへインストールしてください。インストールフォルダの変更が必要な場合には、管理者権限を持ったユーザのみに変更権限が与えられたフォルダを、インストールフォルダとして指定してください。
・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。
・当該製品を使用する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)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可してください。
・当該製品を使用するパソコンを LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックしてください。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしないようにしてください。

CVE-2024-4230

・リアルタイムフローデザイナのプログラム実行フィードバック設定にてプログラムを指定する場合には、信頼できるファイルを指定してください。
・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。
・当該製品を使用する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)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可してください。
・当該製品を使用するパソコンを LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックしてください。
・信頼できないファイル(特にプロジェクトファイル)を開いたり、信頼できないリンクをクリックしないようにしてください。

■お客様からのお問い合わせ先
脆弱性に関するお問い合わせは下記窓口までご連絡ください。
Email:PSIRT@edgecross.org