Edgecross 基本ソフトウェア Windows 版における複数の脆弱性

公開日 2023 年 3 月 2 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 1.10 以降にサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、細工したパケットを送信することにより当該製品をサービス停止(DoS)状態に陥らせることができます。

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-2022-0778	CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
CVE-2022-29862	CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
CVE-2022-29864	CVSS v3.1	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通りです。また、マネジメントシェルのサービスを明示的に止めていない場合に脆弱性の影響を受けます。

製品	形名	バージョン
Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W	1.10～1.26
開発者用 Edgecross 基本ソフトウェア Windows 版	ECP-BS1-W-D	1.10～1.26

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 マネジメントシェルエクスプローラを起動し、「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)

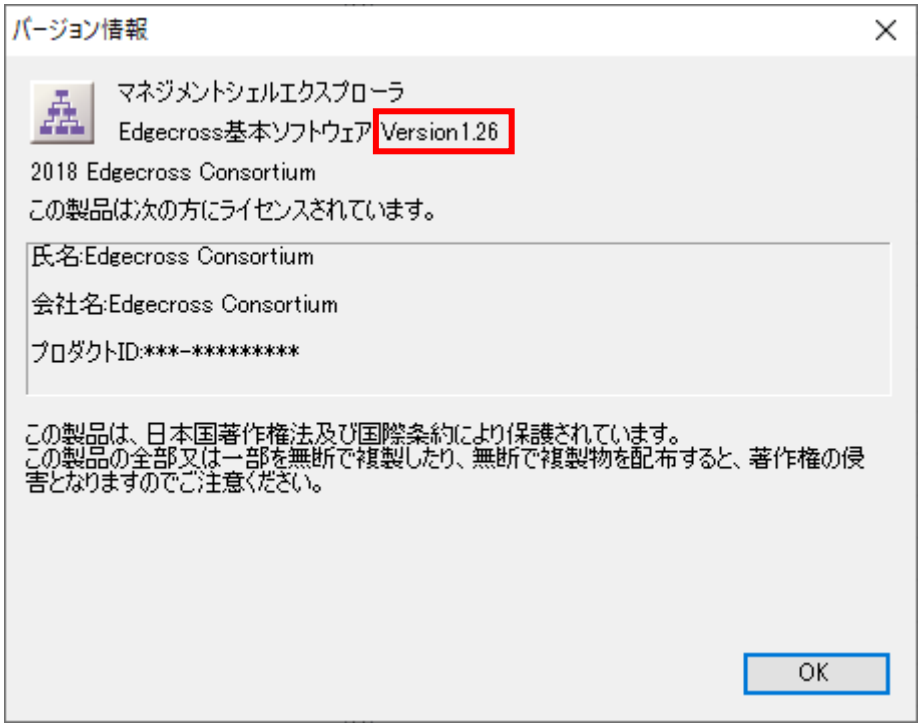

図 1:Edgecross 基本ソフトウェア Windows 版 バージョン情報画面(マネジメントシェルエクスプローラ)

■脆弱性の説明

以下に示す問題により、当該製品がサービス停止(DoS)状態に陥る可能性があります。

・CVE-2022-0778:　無限ループ(CWE-835)
・CVE-2022-29862: 無限ループ(CWE-835)
・CVE-2022-29864: リソースの枯渇(CWE-400)

■脆弱性がもたらす脅威

攻撃者は、細工したパケットを送信することにより当該製品をサービス停止(DoS)状態に陥らせることができます。

■対策方法

下記サイトよりログインの上、Edgecross 基本ソフトウェアバージョン 1.27 以降をダウンロードし、アップデートしてください。

https://www.edgecross.org/member/ja/login.html

※ダウンロードには、事前のユーザ登録が必要です。

ユーザ登録フォーム:https://forms.office.com/r/gKTNxi76P7

■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、以下に示す軽減策を講じることを推奨します。

・当該製品をインターネットに接続する場合には、仮想プライベートネットワーク等を使用し、不正アクセスを防止してください。
・当該製品を LAN 内で使用し、信頼できないネットワークやホストとの通信をファイアウォールでブロックしてください。
・当該製品を使用するパソコンおよび同一ネットワーク機器への物理的なアクセスを制限してください。

■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