Multiple Malicious Program Execution Vulnerabilities in Edgecross Basic Software for Windows

Release date: November 21, 2024
Last update date: November 21, 2024
Edgecross Consortium

■Overview

Multiple malicious program execution vulnerabilities have been discovered in versions 1.00 and later of Edgecross Basic Software for Windows. If these vulnerabilities are exploited by a malicious attacker, there is a possibility that a malicious program will be executed to obtain, tamper, destroy, or delete information. It may also cause a Denial of Service (DoS) on the target.

The affected versions of Edgecross Basic Software for Windows are listed below. Please apply the measures described in the mitigation steps for the respective product.

■CVSS

CVE-2024-4229 CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H Base Score:7.8
CVE-2024-4230 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score:7.8

■Affected products

The affected products are as follows:

・CVE-2024-4229

The vulnerability only affects users who install the product by specifying a folder without administrator privileges.

Products		Type	Version
Edgecross Basic Software for Windows		ECP-BS1-W	1.00 or later
Edgecross Basic Software for Developers		ECP-BS1-W-D	1.00 or later

・CVE-2024-4230

Products	Type	Version
Edgecross Basic Software for Windows	ECP-BS1-W	1.00 or later
Edgecross Basic Software for Developers	ECP-BS1-W-D	1.00 or later

Here is how to comfirm the version number you're using:

1. Launch the Real-time Flow Designer of Edgecross Basic Software for Windows by selecting "Version Information" from the "Help" menu.
2. The version number of the running Edgecross Basic Software for Windows can be found in the following section of the displayed window. (Refer to Figure 1)

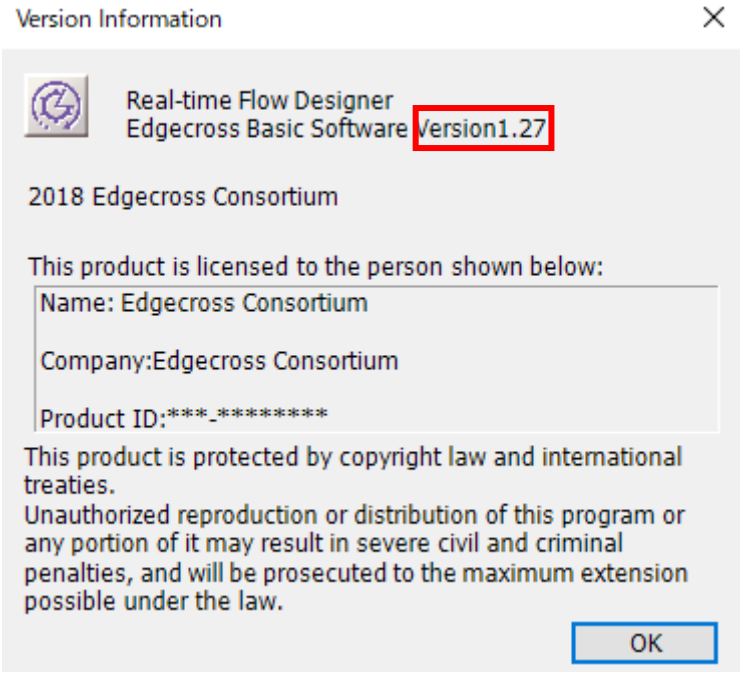

Figure 1: Edgecross Basic Software for Windows Version Information Screen (Real-time Flow Designer)

■Description

Due to the following issues, there is a possibility of the malicious program execution in this product.

・CVE-2024-4229: Incorrect Default Permissions (CWE- 276)

・CVE-2024-4230: External Control of File Name or Path (CWE-73)

■Impact

If these vulnerabilities are exploited by a malicious attacker, there is a possibility that a malicious program will be executed to obtain, falsify, destroy, delete information, or cause a Denial of Service (DoS) on the target.

■Countermeasures

Please take a Mitigations.

■Mitigations

We recommend that you take the following mitigations to minimize the risk of these vulnerabilities being exploited:

CVE-2024-4229

・Please install the product in the default installation folder. If you need to change the installation folder, specify a folder that only users with administrator privileges have permission to change.

・Please install antivirus software on the computer that uses the product.

・When connecting the product to the Internet, use a firewall or virtual private network (VPN) to prevent unauthorized access, and then allow only trusted users to log in remotely.

・Please use the computer using the product within the LAN and block remote login from untrusted networks, hosts, and users.

・Avoid opening untrusted files or clicking on untrusted links.

CVE-2024-4230

・When specifying a program in the real-time flow designer's program execution feedback settings, please specify a reliable file.

・Please install antivirus software on the computer that uses the product.

・When connecting the product to the Internet, use a firewall or virtual private network (VPN) to prevent unauthorized access, and then allow only trusted users to log in remotely.

・Please use the computer using the product within the LAN and block remote login from untrusted networks, hosts, and users.

・Avoid opening untrusted files or clicking on untrusted links.

■Contact information

Please contact the receptionist below for any questions.

email:PSIRT@edgecross.or