Multiple vulnerabilities in Edgecross Basic Software for Windows

Release date: March 2,2023
Edgecross Consortium

■Overview

It is confirmed that vulnerabilities of Denial-of-Service (DoS) exist in Edgecross Basic Software for Windows (version from 1.10). An attacker can exploit the vulnerabilities to cause the Denial-of-Service (DoS) condition by sending a crafted packet.

Versions of the Edgecross Basic Software for Windows affected by these vulnerabilities are listed below.

■CVSS

CVE-2022-0778	CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5
CVE-2022-29862	CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5
CVE-2022-29864	CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5

■Affected products

The affected product and versions are below. Furthermore, these vulnerabilities influence the products unless Management Shell seivece has been stopped manually.

products	Module Name	versions
Edgecross Basic Software for Windows	ECP-BS1-W	1.10 to 1.26
Edgecross Basic Software for Developers	ECP-BS1-W-D	1.10 to 1.26

How to check the version number you're using is below.

1.Start Edgecross Basic Software for Windows Management Shell Explorer and select "Version Information" form the "Help" menu.

2.The following part of the window that appears is the version number of Edgecross Basic Software for Windows.(See Figure 1)

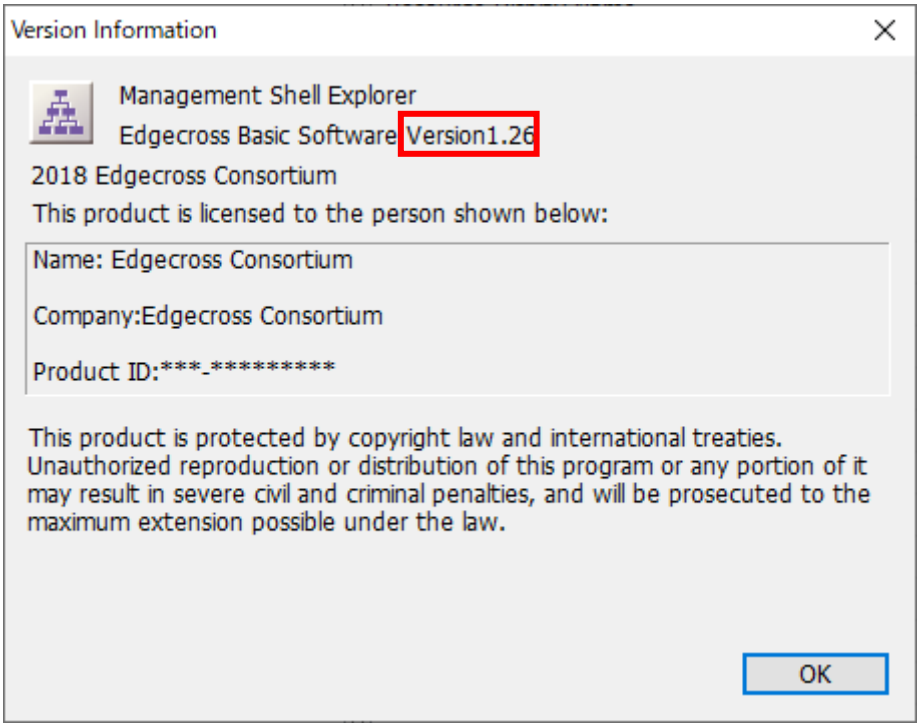

Figure 1: Edgecross Basic Software for Windows(Management Shell Explorer) Version Information Window

■Description

The following issues can cause a denial of service (DoS) condition on the affected product:

CVE-2022-0778: Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835)

CVE-2022-29862: Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835)

CVE-2022-29864: Uncontrolled Resource Consumption (CWE-400)

■Impact

An attacker can exploit the vulnerabilities to cause a Denial-of-Service (DoS) condition by sending a crafted packet.

■Countermeasures

Login the following URL and, download the fixed version of Edgecross Basic Software Version 1.27.
Then, install it on a personal computer.

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

※Prior user registration is required to download.
For inquiries about user registration, please contact the following email address.
email:user.registration@edgecross.org

■Mitigations

Recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:

・When Internet access is required, use a virtual private network (VPN) or other means to prevent unauthorized access.
・Use the products within a LAN and block access from untrusted networks and hosts.
・Restrict physical access to your computer with the products installed and network equipment on the same network.

■Contact information

Please contact the receptionist below for any questions.
email:PSIRT@edgecross.org