Malicious Code Execution Vulnerability in MELIPC Series MI5122-VW

Release date: July 4, 2024
Mitsubishi Electric Corporation

Overview

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE-276[1]) exists in Smart Device Communication Gateway preinstalled on MELIPC Series MI5122-VW. A local attacker may execute arbitrary code by saving a malicious file to a specific folder. As a result, the attacker may disclose, tamper with, destroy or delete information in the product, or cause a denial-of-service (DoS) condition on the product. (CVE-2024-3904)
The product models and versions affected by this vulnerability are listed below.

CVSS[2]

CVE-2024-3904 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H Base Score: 8.8

Affected products

The affected products are as follows:

Series	Model name	Version
MELIPC Series	MI5122-VW	Firmware versions "05" to "07"

Please refer to the following user's manual for how to check the firmware version.
・MELIPC MI5000 Series User's Manual (Startup) "Appendix 17 Checking Production Information and Firmware Version"

The manuals for our products are available for download from the following website.
https://www.mitsubishielectric.com/fa/download/index.html

Description

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE-276) exists in Smart Device Communication Gateway preinstalled on MELIPC Series MI5122-VW.

Impact

A local attacker may execute arbitrary code by saving a malicious file to a specific folder. As a result, the attacker may disclose, tamper with, destroy or delete information in the product, or cause a denial-of-service (DoS) condition on the product.

Countermeasures for Customers

<Customers using the affected MELIPC Series product>

Customers who are using an affected version of the affected product should take measures described in Workarounds section and Mitigations section.
We have released the fixed version as shown below, but updating the product to the fixed version is not available.

Countermeasures for Products

The following products have been fixed to prevent incorrect default permissions from being set.

Series	Model name	Version
MELIPC Series	MI5122-VW	Firmware versions "08" or later

[1] https://cwe.mitre.org/data/definitions/276.html

[2] https://www.first.org/cvss/v3.1/specification-document

Workarounds

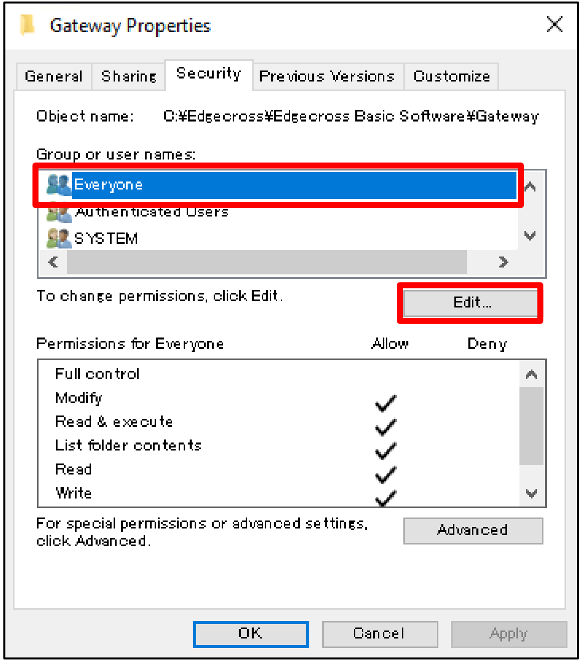
Please check the access permissions for the target folders and remove the permission for Everyone by following the procedure below.

[Target folders]
C:/Edgecross/Edgecross Basic Software/Gateway
C:/Edgecross/Edgecross Basic Software/Gateway/ITGWMDA_000002_SDCommGateway
C:/Edgecross/Edgecross Basic Software/Gateway/ITGWMDA_000002_SDCommGateway/settings
C:/Edgecross/Edgecross Basic Software/Gateway/ITGWMDA_000002_SDCommGateway/icon
C:/Edgecross/Edgecross Basic Software/Gateway/ja-JP
C:/Edgecross/Edgecross Basic Software/Gateway/zh-CN
C:/Edgecross/Edgecross Basic Software/Gateway/ITGWMDA_000002_SDCommGateway/Doc

[Procedure]

(1) Right-click the target folder and select **Properties**.

(2) Select the **Security** tab, and if Everyone exists, click the **Edit** button.
(If Everyone does not exist, there is no problem and the procedure ends.)



Gateway Properties

Object name: C:¥Edgecross¥Edgecross Basic Software¥Gateway

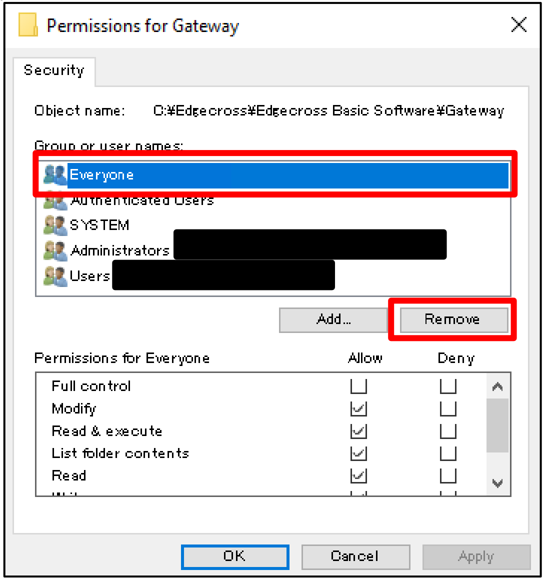
Group or user names:
Everyone
Authenticated Users
SYSTEM

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

(3) Select Everyone and click the **Remove** button.



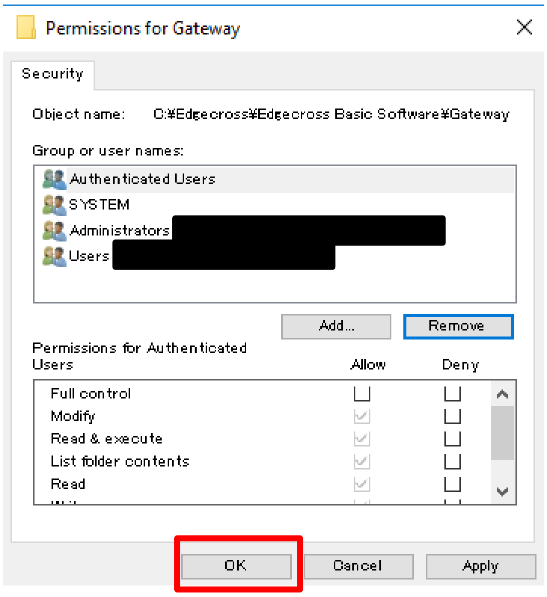
Permissions for Gateway

Object name: C:¥Edgecross¥Edgecross Basic Software¥Gateway

Group or user names:
Everyone
Authenticated Users
SYSTEM
Administrators [redacted]
Users [redacted]

Permissions for Everyone	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

(4) Click the **OK** button to close the Permissions window.



Permissions for Gateway

Security

Object name: C:¥Edgecross¥Edgecross Basic Software¥Gateway

Group or user names:

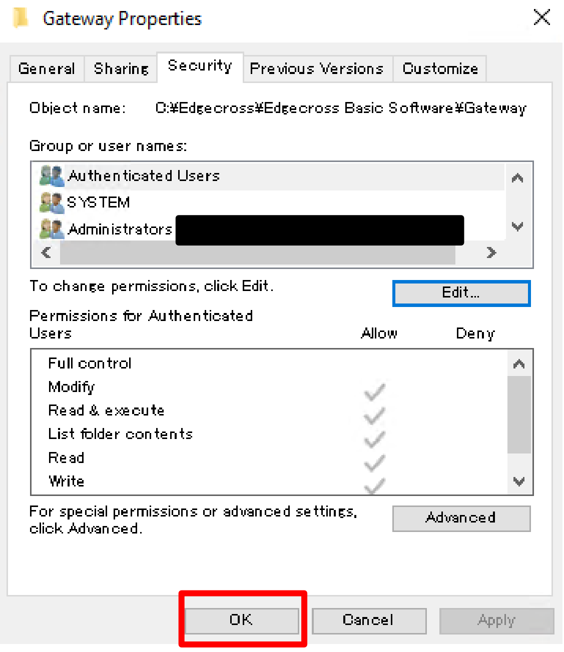
- Authenticated Users
- SYSTEM
- Administrators [redacted]
- Users [redacted]

Add... Remove

Permissions for Authenticated Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

OK Cancel Apply

(5) Click the **OK** button to close the Properties window.



Gateway Properties

General Sharing Security Previous Versions Customize

Object name: C:¥Edgecross¥Edgecross Basic Software¥Gateway

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators [redacted]

To change permissions, click Edit. Edit...

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

Mitigations

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of this vulnerability being exploited:

- Install an antivirus software on the affected product.
- Restrict physical access to the affected product and the LAN to which the affected product is connected.
- Use the affected product within the LAN and block remote login from untrusted networks, hosts, and users.
- When connecting the affected product to the internet, use a firewall, virtual private network (VPN), etc., to prevent unauthorized access, and allow only trusted users to remotely log on.
- Do not open untrusted files or click untrusted links.

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html