# Malicious Code Execution Vulnerability in Mitsubishi Small-Capacity UPS Shutdown Software FREQSHIP-mini for Windows

Release date: February 3, 2026
Mitsubishi Electric Corporation

## Overview

Malicious code execution vulnerability due to Incorrect Default Permissions (CWE-276[1]) exists in Mitsubishi small-capacity UPS shutdown software FREQSHIP-mini for Windows. A local attacker may be able to execute arbitrary code with system privileges by replacing service executable files (EXE) or DLLs in the installation directory with specially crafted files. As a result, the attacker may be able to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a Denial of Service (DoS) condition on the affected system (CVE-2025-10314).

## CVSS[2]

CVE-2025-10314 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:

| Product Name | Version |
|---|---|
| FREQSHIP-mini for Windows | 8.0.0 - 8.0.2 |

<How to check the version>
Refer to the “Ver.” notation displayed on the UPS environment settings screen when the product is launched.

## Description

Malicious code execution vulnerability due to Incorrect Default Permissions (CWE-276) exists in Mitsubishi small-capacity UPS shutdown software FREQSHIP-mini for Windows.

## Impact

A local attacker may be able to execute malicious code with system privileges by replacing service executable files (EXE) or DLLs in the installation directory with specially crafted files. As a result, the attacker may be able to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a Denial of Service (DoS) condition on the affected system.

## Countermeasures for Customers

<For customers using Windows 10, Windows 11, or Windows Server 2022>
Please download and install the latest version of the product from the following site:
https://www.mitsubishielectric.co.jp/fa/download/index.html (In Japanese)

<For customers using Windows Vista, Windows 7, Windows 8, Windows 8.1, or Windows Server 2008>
There are no plans to release a fixed version, so please take the following mitigations / workarounds.

## Countermeasures for Products

The vulnerability has been fixed in the following version:

| Product Name | Version |
|---|---|
| FREQSHIP-mini for Windows | 8.1.0 or later |

## Mitigations / Workarounds

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

- Use the PCs with the affected product installed only within a LAN, and block remote logins from untrusted networks, hosts, and non-administrator users.
- Block unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to administrator when connecting the PCs with the affected product installed to the internet.
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.

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

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

- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.
- Install antivirus software on the PC with the affected product installed.

## Acknowledgement

Mitsubishi Electric would like to thank Kazuma Matsumoto, Security Researcher at GMO Cybersecurity by IERAE, Inc., who reported this vulnerability.

## Contact information

Please contact your local Mitsubishi Electric representative.
<Contact | MITSUBISHI ELECTRIC>
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html (In Japanese)