Information Tampering Vulnerability in Multiple Processes of GENESIS64, MC Works64, and GENESIS

Release date: August 5, 2025
Mitsubishi Electric Corporation

Overview

An information tampering vulnerabilitiy exists in multiple processes of GENESIS64, MC Works64, and GENESIS. An attacker could make an unauthorized write to arbitrary files, by creating a symbolic link from a file used as a write destination by the processes of GENESIS64, MC Works64, and GENESIS to a target file. This could allow the attacker to destroy the file on a PC with GENESIS64, MC Works64, and GENESIS installed (CVE-2025-7376), resulting in a denial-of-service (DoS) condition on the PC.

Affected versions of GENESIS64, MC Works64, and GENESIS are listed below. Please take mitigation measures described in the "Countermeasures for Customers" section.

CVSS[1]

CVE-2025-7376 CVSS:v3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N Base Score: 5.9

Affected products

<Affected products and versions>
- GENESIS64 all versions
- MC Works64 all versions
- GENESIS: Version 11.00

<How to check GENESIS version (Windows 11)>
Open the Settings and select Apps > Apps & features.
It is applicable if the version displayed in “ICONICS GENESIS” is “11.0.812” (Figure. 1).

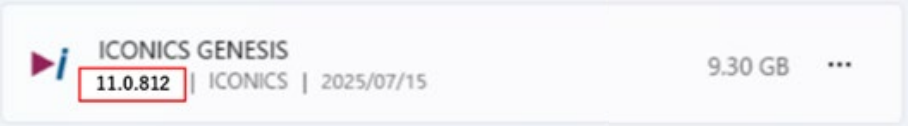

Figure 1 GENESIS Version11.00

Description

An information tampering vulnerability due to Windows Shortcut Following (.LNK) (CWE-64[2]) exists in multiple processes in GENESIS64, MC Works64, and GENESIS.

Impact

An attacker could make an unauthorized write to arbitrary files, by creating a symbolic link from a file used as a write destination by the processes of GENESIS64, MC Works64, and GENESIS to a target file. This could allow the attacker to destroy the file on a PC with GENESIS64, MC Works64, and GENESIS installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC if the destroyed file is necessary for the operation of the PC.

Countermeasures for Customers

<Customers using MC Works64>
There are no plans to release a fixed version, so we kindly ask you to take the mitigations described in "Mitigations".

<Customers using GENESIS64>
We are currently developing a fixed version and going to release it in the near future.
Please take the mitigations described in "Mitigations" until it is released.

<Customers using GENESIS>
Please download and apply the latest GENESIS described in “Countermeasures for Products.”

Countermeasures for Products

<MC Works64>
There are no plans to release a fixed version.

---

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

[2] https://cwe.mitre.org/data/definitions/64.html

< GENESIS64>
We are currently developing a fixed version.

<GENESIS>
The version that includes countermeasures against this vulnerability is as follows.

・ GENESIS Version 11.01 or later
Please download the latest version from the link below.
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

Mitigations

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability.

1) Please configure the PCs with the affected product installed so that only an administrator can log in.
2) Use the PCs with the affected product installed in the LAN and block remote login from untrusted networks and hosts, and from non-administrator users.
3) 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.
4) 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.
5) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>
https://www.mitsubishielectric.com/fa/support/index.html