Information Tampering Vulnerability in Multiple Services of GENESIS64, ICONICS Suite, MC Works64, GENESIS, GENESIS32, and BizViz

Release date: May 15, 2025
Last update date: January 8, 2026
Mitsubishi Electric Corporation

Overview

An information tampering vulnerabilitiy exists in multiple services of GENESIS64, ICONICS Suite, MC Works64, GENESIS, GENESIS32, and BizViz. A local attacker could make an unauthorized write to arbitrary files, by creating a symbolic link from a file used as a write destination by the services of the affected products to a target file. This could allow the attacker to destroy the file on a PC with the affected products installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC.

Affected versions of GENESIS64, ICONICS Suite, MC Works64, GENESIS, GENESIS32, and BizViz are listed below. Please take mitigation measures described in the "Countermeasures for Customers" section.

CVSS[1]

CVE-2025-0921 CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N Base Score: 6.5

Affected products

<Affected products and versions>

- GENESIS64, ICONICS Suite, MC Works64, GENESIS32, and BizViz: 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).

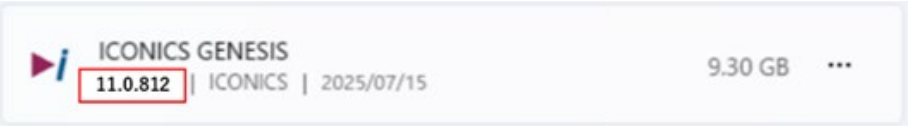

Figure 1 GENESIS Version11.00

Description

An information tampering vulnerability due to Execution with Unnecessary Privileges (CWE-250[2]) exists in multiple services in GENESIS64, ICONICS Suite, MC Works64, GENESIS, GENESIS32, and BizViz.

Impact

A local attacker could make an unauthorized write to arbitrary files, by creating a symbolic link from a file used as a write destination by the services of affected products to a target file. This could allow the attacker to destroy the file on a PC with affected products 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, GENESIS32, and BizViz>
There are no plans to release a fixed version, so we kindly ask you to take the mitigations described in "Mitigations".
To minimize the risk of this vulnerability being exploited, please consider replacing it with GENESIS64 or its successor product, GENESIS.

<Customers using GENESIS64 and ICONICS Suite>
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.”

---

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

[2] https://cwe.mitre.org/data/definitions/250.html

Countermeasures for Products

<MC Works64, GENESIS32, and BizViz>
There are no plans to release a fixed version.

<GENESIS64 and ICONICS Suite>
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 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.

Acknowledgement

Mitsubishi Electric would like to thank Asher Davila and Malav Vyas, Security Researchers at Palo Alto Networks, who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

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

Update history

January 8, 2026
Revised Title, Overview, Affected products, Description, Countermeasure for Customers, and Countermeasures for Products.
Added ICONICS Suite, GENESIS32, and BizViz to Affected products.

September 18, 2025
Revised Overview and Impact.

August 5, 2025
Revised Title, Overview, Affected products, Description, Impact, Countermeasure for Customers, Countermeasures for Products, and Mitigations.
Added GENESIS to Affected products.