Information Tampering Vulnerability in Multiple Processes of GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, IoTWorX, MC Works64, and GENESIS

Release date: August 5, 2025
Last update date: April 7, 2026
Mitsubishi Electric Corporation

Overview

An information tampering vulnerabilitiy exists in multiple processes of GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, IoTWorX, MC Works64, and GENESIS. 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 processes 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, resulting in a denial-of-service (DoS) condition on the PC (CVE-2025-7376).

Affected versions of GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, IoTWorX, 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 Version 10.97.3 and prior
- ICONICS Suite Version 10.97.3 and prior
- MobileHMI Version 10.97.3 and prior
- Hyper Historian Version 10.97.3 and prior
- AnalytiX Version 10.97.3 and prior
- IoTWorX Version 10.95
- MC Works64 all versions
- GENESIS Version 11.00

<How to check GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, and IoTWorX version>
Open Windows Control Panel and select "Programs and Features".
It is applicable if the version displayed for the affected product* is “10.97.305.55” or prior (Figure. 1).
*Versions 10.96.2 or later of GENESIS64, MobileHMI, Hyper Historian, AnalytiX, and IoTWorX are bundled with the ICONICS Suite installer, so the product name appears as "ICONICS Suite".

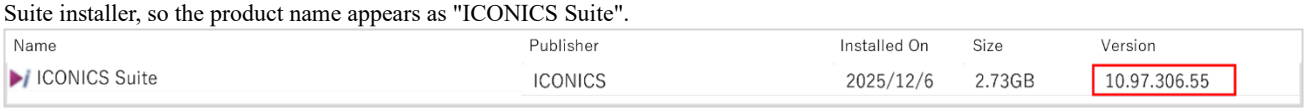

Figure 1 GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX Version 10.97.3

<How to check GENESIS version>
Open Windows Control Panel and select "Programs and Features".
It is applicable if the version displayed in “ICONICS GENESIS” is “11.0.812” (Figure. 2).

Figure 2 GENESIS Version 11.00

<How to check IoTWorX version>
Open Windows Control Panel and select "Programs and Features".
It is applicable if the version displayed for “ICONICS IoTWorX Gateway” is “10.95.198.44” (Figure. 3).

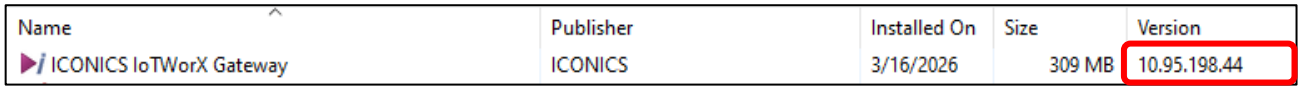

Figure 3 IoTWorX Version 10.95

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

Description

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

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 processes of GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, IoTWorX, MC Works64, and GENESIS to a target file. This could allow the attacker to destroy the file on a PC with the affected products installed, 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, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, and IoTWorX>
Please download and install the latest product described in “Countermeasures for Products.”

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

Countermeasures for Products

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

<GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX >
The version that includes countermeasures against this vulnerability is as follows.
・ ICONICS Suite Version 10.98 or later
Please download from the link below.
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads?tabset-a9d51=51905

*GENESIS64, MobileHMI, Hyper Historian, AnalytiX, and IoTWorX are included in the ICONICS Suite installation.

<IoTWorX>
The version that includes countermeasures against this vulnerability is as follows.
・ IoTWorX Version 10.96 or later
Please download from the link below.
https://iconicsinc.my.site.com/community/s/iconics-software/a375a000004qDU8AAM/iotworx

<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/service-support/index.html

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

Update history

April 7, 2026

Revised Title, Overview, Affected products, Description, Impact, Countermeasure for Customers, and Countermeasures for Products.

Added MobileHMI, Hyper Historian, AnalytiX, and IoTWorX to Affected products.

September 18, 2025

Revised Overview and Impact.