Information Tampering Vulnerability in Multi-agent Notification Feature of GENESIS64^{TM} and MC Works64

Release date: May 15, 2025
Mitsubishi Electric Corporation

Overview

A information tampering vulnerabilitiy exists in multi-agent notification feature of GENESIS64^{TM} and MC Works64. 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 services of GENESIS64^{TM} and MC Works64 to a target file. This could allow the attacker to destroy the file on a PC with GENESIS64^{TM} and MC Works64 installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC.

Affected versions of GENESIS64^{TM} and MC Works64 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^{TM} all versions
- MC Works64 all versions

Description

A information tampering vulnerability due to Execution with Unnecessary Privileges (CWE-250[2]) exists in the Pager agent of multi-agent notification feature in GENESIS64^{TM} and MC Works64.

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 services of GENESIS64^{TM} and MC Works64 to a target file. This could allow the attacker to destroy the file on a PC with GENESIS64^{TM} and MC Works64 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 GENESIS64^{TM} and MC Works64>

Mitsubishi Electric is currently preparing a fixed version for this vulnerability. In the meantime, please take the following mitigation measures.

Countermeasures for Products

< GENESIS64^{TM} and MC Works64>

Mitsubishi Electric is currently preparing a fixed version for this vulnerability.

Mitigations

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

1) If you do not need to use the multi-agent notification feature, please uninstall it. The multi-agent notification feature is not included in the default installation of GENESIS64^{TM} version 10.97.3 or later.
   For customers who need to use the multi-agent notification feature, and do not need to use the Pager agent, please execute a custom installation of the multi-agent notification feature and skip the installation of the Pager agent.
2) Please configure the PCs with the affected product installed so that only an administrator can log in.
3) 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.
4) 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.
5) 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.
6) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

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

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

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

Trademarks

GENESIS64^{TM} is a trademark of Mitsubishi Electric Iconics Digital Solutions, Inc.