

**Whitepaper on  
GENESIS v11  
Security  
Vulnerabilities  
(April 2026)**





## Contents

1	Introduction.....	4
2	Information Tampering Vulnerability in GENESIS v11 Classic OPC Point Manager Service (ICSA-25-140-04)...	5
3	Information Tampering Vulnerability in GENESIS v11 Processes (ICSA-25-217-01).....	6
4	Cleartext Storage of SQL Password (ICSA-26-097-01) .....	7

## Copyright and Confidentiality

This document contains proprietary information of Mitsubishi Electric Iconics Digital Solutions, Inc. and is subject to the condition that no copy or other reproduction be made in whole or in part for any use. No use may be made of information herein except for which it is transmitted, without the express written consent of Mitsubishi Electric Iconics Digital Solutions, Inc.

Copyright © Mitsubishi Electric Iconics Digital Solutions, Inc. All rights reserved.

Revision	1.1
Issued	April 7, 2026

# 1 Introduction

Mitsubishi Electric Iconics Digital Solutions takes extraordinary efforts in testing and validating its software before it is released. Unfortunately, there are instances where security vulnerabilities are discovered, either internally, or by external researchers. Mitsubishi Electric Iconics Digital Solutions takes such issues very seriously. All such vulnerabilities are documented, assigned to engineering teams for investigation and validation, and addressed as quickly as reasonably possible. Once fully tested, software updates for the current release and, in some cases, past releases, are posted to the company's Community Portal. Information on the updates is provided on the following website:

[Security at ICONICS | ICONICS Software Solutions](#)

Mitsubishi Electric Iconics Digital Solutions coordinates with the US government's Cybersecurity & Infrastructure Security Agency (CISA), as well as its parent company, Mitsubishi Electric, on these issues. The following table is a summary of what updates are necessary to bring the given version as up to date as possible with regards to protecting the system against the vulnerabilities described in this document..

<b>GENESIS software version</b>	<b>Is not subject to these vulnerabilities...</b>	<b>...After applying this update or these patch files...</b>
<b>11.03</b>	Sections 2-4	None required
<b>11.01</b>	Sections 2-3	None required

Mitsubishi Electric Iconics Digital Solutions recommends that users of its products (GENESIS):

- Use a firewall. Place control system networks, devices, and SCADA system components behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Use a VPN for remote access to control system devices.

Acronyms and Terms used in this document:

<b>Term</b>	<b>Definition</b>
<b>CISA</b>	Cybersecurity & Infrastructure Security Agency
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>CVSS</b>	Common Vulnerability Scoring System
<b>CWE</b>	Common Weakness Enumeration
<b>DoS</b>	Denial of Service
<b>ICSA</b>	Industrial Control Systems Advisory
<b>NIST</b>	National Institute of Standards and Technology
<b>OPC</b>	Open Platform Communications
<b>OPC UA</b>	Open Platform Communications Unified Architecture

## 2 Information Tampering Vulnerability in GENESIS v11 Classic OPC Point Manager Service (ICSA-25-140-04)

### 2.1 Date : August 2025

### 2.2 Issue – Discussion

An information tampering vulnerability exists in a GENESIS v11 service, the one providing classic OPC server communications. 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 Classic OPC Point Manager service of GENESIS v11 to a target file. This could allow the attacker to destroy the file on a PC with GENESIS installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC.

### 2.3 Products Affected

Product	Version	Security Impact	CWE	CVE
GENESIS v11	v11.00	Unauthorized write to arbitrary files	250 – Execution with Unnecessary Privileges	CVE-2025-0921

**CVSS V3.1 Base Score:** 6.5 (AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N)

### 2.4 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 GENESIS v11 Classic OPC Server communications service. This could allow the attacker to destroy the file on a PC with 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.

### 2.5 Mitigations

Mitsubishi Electric Iconics Digital Solutions recommends updating the following to the latest versions:

- GENESIS: Versions 11.01 or later

The GENESIS version 11.00 installation by default will disable the service for Classic OPC Point Manager service. It is recommended that GENESIS v11.00 users upgrade to version 11.01 or later, and to not enable the Classic OPC Point Manager Service.

GENESIS v11.00 users who have the Classic OPC Point Manager service enabled should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Configure the PCs with the affected product installed so that only an administrator can log in.
- PCs with the affected product installed should be configured to block remote logins from untrusted networks and hosts, and from non-administrator users.
- Block unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to administrators 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.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 3 Information Tampering Vulnerability in GENESIS v11 Processes (ICSA-25-217-01)

### 3.1 Date : August 2025

### 3.2 Issue – Discussion

An information tampering vulnerability due to Windows Shortcut Following (.LNK) (CWE-64 ) exists in multiple processes in GENESIS v11. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. By creating a symbolic link, an attacker can cause the processes to make unauthorized writes into arbitrary files on the file system in any location that is accessible to the user under which the elevated processes are running (CVE-2025-7376), resulting in a denial-of-service (DoS) condition on the PC if the modified file is necessary for the operation of the PC.

### 3.3 Products Affected

Product	Version	Security Impact	CWE	CVE
GENESIS v11	v11.00	Unauthorized write to arbitrary files	64 – Windows Shortcut Following (.LNK)	CVE-2025-7376

**CVSS V3.1 Base Score:** 5.9 (AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N)

### 3.4 Impact

By creating a symbolic link, an attacker can cause the processes to make unauthorized writes into arbitrary files on the file system in any location that is accessible to the user under which the elevated processes are running (CVE-2025-7376), resulting in a denial-of-service (DoS) condition on the PC if the modified file is necessary for the operation of the PC.

### 3.5 Mitigations

GENESIS version 11.01 contains the fix for this vulnerability. For the highest level of security, it is recommended that users upgrade their system to the latest version and keep it up-to-date with the latest releases. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

GENESIS v11.00 users who remain on this version should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Configure the PCs with the affected product installed so that only an administrator can log in.
- PCs with the affected product installed should be configured to block remote logins from untrusted networks and hosts, and from non-administrator users.
- Block unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to administrators 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.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 4 Cleartext Storage of SQL Password (ICSA-26-097-01)

**4.1 Date:** April 2026

### 4.2 Issue – Discussion

Multiple information disclosure, tampering, and Denial-of-Service (DoS) vulnerabilities exist in GENESIS. When the local cache (SQLite) feature of affected products is enabled and the SQL Server authentication method is SQL authentication, an attacker may be able to disclose SQL Server credentials stored on the PC where the product is installed (CVE-2025-14815). And, when the SQL Server authentication method is SQL authentication, an attacker may be able to disclose SQL Server credentials from the screen of affected products (CVE-2025-14816). As a result, the attacker could access the SQL Server illegally to disclose data, tamper with or destroy data, and cause a denial-of-service (DoS) condition on the system.

The versions of products affected by these vulnerabilities are listed below. Please implement the measures described in the “Mitigations” section.

### 4.3 Products Affected

<Affected products and versions>

GENESIS : Version 11.02 and prior

The products and versions listed above are affected by the following vulnerabilities:

Security Impact	CVSS	CWE	CVE
Information disclosure, tampering, and Denial-of-Service (DoS)	9.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)	Cleartext Storage of Sensitive Information (CWE-312)	CVE-2025-14815
Information disclosure, tampering, and Denial-of-Service (DoS)	9.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)	Cleartext Storage of Sensitive Information in GUI (CWE-317)	CVE-2025-14816

### 4.4 Impact

An attacker may be able to disclose the SQL Server credentials used by the affected products by exploiting these vulnerabilities. As a result, the unauthorized attacker could access the SQL Server and disclose, tamper with, or destroy data on the server, potentially cause a denial-of-service (DoS) condition on the system.

### 4.5 Mitigation

GENESIS Version 11.03 and later is not vulnerable to these vulnerabilities. Affected customers should upgrade to one of these versions to obtain the fix for these vulnerabilities.

For affected users who are unable to upgrade, Mitsubishi Electric Iconics Digital Solutions recommends that users of its products take the following mitigation steps:

- Use Windows authentication instead of SQL authentication for the SQL server authentication method.
- Restrict access to the affected GENESIS machine only to administrators.

- Install an antivirus software in your computer using the affected product.
- Don't open files from untrusted sources.
- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click web links or open unsolicited attachments in e-mail messages.
- Install any applicable Critical Fixes Rollup, if available.

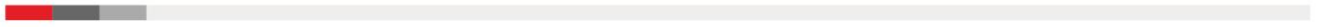
#### CVE-2025-14815

- 1) In Workbench, open the "Configure Application(s) Settings" dialog. In the "Available Applications" list, uncheck the "Local Cache" column for applications and delete the files created by the local cache functionality from the following location:  
C:\ProgramData\ICONICS\11\Cache\\*.sqlite3

#### CVE-2025-14816

- 1) Change the permissions of HHSplitter.exe so that only trusted administrators can execute it.
- 2) Delete HHSplitter.exe from the system if it is unnecessary.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.



## About Us

Mitsubishi Electric Iconics Digital Solutions, headquartered in Foxborough, Massachusetts, is a global leader in industrial automation, smart and sustainable buildings, and digitalization software. Our advanced HMI, SCADA, and Smart Building solutions enable businesses to visualize, monitor, and optimize their most critical assets and spaces. With installations in over 100 countries and adoption by more than 70% of Global 500 companies, we drive operational efficiency and continuous improvement across industrial manufacturing, infrastructure, and built environment sectors. Backed by cutting-edge technology and deep industry expertise, we deliver flexible, scalable, and high-performance software solutions. As a testament to our excellence, Mitsubishi Electric Iconics Digital Solutions has been recognized as a seven-time winner of the Microsoft Partner of the Year award.

## Mitsubishi Electric Iconics Digital Solutions Sales Offices

**World Headquarters**  
2 Hampshire Street  
Foxborough, MA, USA, 02035  
+1 508 543 8600  
info@iconics.com

<b>Australia</b> australia@iconics.com	<b>France</b> france@iconics.com	<b>Japan</b> japan@iconics.com	<b>Philippines</b> philippines@iconics.com	<b>UK</b> uk@iconics.com
<b>Brazil</b> brazil@iconics.com	<b>Germany</b> germany@iconics.com	<b>Malaysia</b> malaysia@iconics.com	<b>Singapore</b> singapore@iconics.com	<b>Vietnam</b> vietnam@iconics.com
<b>Canada</b> canada@iconics.com	<b>India</b> india@iconics.com	<b>Mexico</b> mexico@iconics.com	<b>South Korea</b> southkorea@iconics.com	
<b>China</b> china@iconics.com	<b>Indonesia</b> indonesia@iconics.com	<b>Middle East</b> middleeast@iconics.com	<b>Taiwan</b> taiwan@iconics.com	
<b>Czech Republic</b> czech@iconics.com	<b>Italy</b> italy@iconics.com	<b>Netherlands</b> holland@iconics.com	<b>Thailand</b> thailand@iconics.com	

## MITSUBISHI ELECTRIC ICONICS DIGITAL SOLUTIONS, INC.

HEAD OFFICE: 2 Hampshire Street, Suite 300, Foxborough, MA 02035