

# Multiple vulnerabilities in GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32 and BizViz

Release date: October 15, 2026  
Mitsubishi Electric Corporation

## Overview

Multiple vulnerabilities exist in, GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32, and BizViz. These vulnerabilities may allow an attacker to execute arbitrary code (CVE-2023-4863), bypass authentication (CVE-2026-16436 and CVE-2026-16437), or perform arbitrary operations (CVE-2026-16438), resulting in information disclosure, tampering with, destruction, or deletion of information, and a denial-of-service (DoS) condition of the system. The versions of products affected by these vulnerabilities are listed below. Please update to the fixed version or take mitigations.

## CVSS<sup>1</sup>

|                |                                                                 |                |
|----------------|-----------------------------------------------------------------|----------------|
| CVE-2023-4863  | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H | Base Score:9.3 |
| CVE-2026-16436 | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N | Base Score:9.2 |
| CVE-2026-16437 | CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N | Base Score:7.1 |
| CVE-2026-16438 | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H | Base Score:9.4 |

## Affected products

The affected products and versions are as follows.

| CVE ID                            | Affected products | Affected versions         |
|-----------------------------------|-------------------|---------------------------|
| CVE-2023-4863                     | GENESIS64         | Version 10.97 to 10.97.2  |
|                                   | ICONICS Suite     | Version 10.97 to 10.97.2  |
| CVE-2026-16436,<br>CVE-2026-16437 | GENESIS           | Version 11.03 and prior   |
|                                   | GENESIS64         | Version 10.97.3 and prior |
|                                   | ICONICS Suite     | Version 10.97.3 and prior |
|                                   | Hyper Historian   | Version 10.97.3 and prior |
|                                   | AnalytiX          | Version 10.97.3 and prior |
|                                   | MobileHMI         | Version 10.97.3 and prior |
|                                   | IoTWorX           | Version 10.97.3 and prior |
|                                   | MC Works64        | All versions              |
|                                   | GENESIS32         | All versions              |
|                                   | BizViz            | All versions              |
| CVE-2026-16438                    | GENESIS64         | Version 10.97.3 and prior |
|                                   | ICONICS Suite     | Version 10.97.3 and prior |
|                                   | Hyper Historian   | Version 10.97.3 and prior |
|                                   | AnalytiX          | Version 10.97.3 and prior |
|                                   | MobileHMI         | Version 10.97.3 and prior |
|                                   | MC Works64        | All versions              |

<How to check the version (Windows 11)>

- 1) Open the Settings and select Apps, and then select Apps & features.
- 2) For customers using GENESIS, it is applicable if the version displayed in “ICONICS GENESIS” is “11.3.578” or prior (Figure. 1).

| Name                                                                                        | Publisher | Installed On | Size    | Version  |
|---------------------------------------------------------------------------------------------|-----------|--------------|---------|----------|
|  GENESIS | ICONICS   | 7/29/2026    | 9.66 GB | 11.3.578 |

Figure 1 GENESIS Version 11.03

- 3) For customers using GENESIS64\* or ICONICS Suite, they are applicable if the version displayed in “ICONICS Suite” is “10.97.020.27” through “10.97.212.46” (Figure. 2).

\* For GENESIS64, please check the “ICONICS Suite” version since it is bundled in the installation.

| Name                                                                                              | Publisher | Installed On | Size    | Version      |
|---------------------------------------------------------------------------------------------------|-----------|--------------|---------|--------------|
|  ICONICS Suite | ICONICS   | 7/27/2026    | 2.53 GB | 10.97.212.46 |

Figure 2 ICONICS Suite Version 10.97.2

<sup>1</sup> <https://www.first.org/cvss/v4-0/specification-document>

- 4) For customers using GENESIS64\*, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, or IoTWorX, they are applicable if the version displayed in “ICONICS Suite” is “10.97.306.55” or prior (Figure. 3).

\* For GENESIS64, MobileHMI, Hyper Historian, and AnalytiX, please check the “ICONICS Suite” version since it is bundled in the installation.

| Name          | Publisher | Installed On | Size   | Version      |
|---------------|-----------|--------------|--------|--------------|
| ICONICS Suite | ICONICS   | 2025/12/6    | 2.73GB | 10.97.306.55 |

Figure 3 ICONICS Suite Version 10.97.3

## Description

The following four vulnerabilities exist in GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32, and BizViz.

| CVE ID         | Description of the vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2023-4863  | An arbitrary code execution vulnerability due to an Out-of-bounds Write (CWE-787) <sup>2</sup> caused by libwebp, an internal component, exists in GENESIS64 and ICONICS Suite.                                                                                                                                                                                                                                                                                                                             |
| CVE-2026-16436 | An authentication bypass vulnerability due to Weak Password Recovery Mechanism for Forgotten Password (CWE-640) <sup>3</sup> exists in GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS 32, and BizViz. In the security challenge feature of the affected products, the challenge response used to unlock the system is common to all users and fixed. Therefore, anyone who obtains the challenge response can unlock the system.                     |
| CVE-2026-16437 | An authentication bypass vulnerability due to Weak Password Recovery Mechanism for Forgotten Password (CWE-640) exists in GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS 32, and BizViz. In the security challenge feature of the affected products, administrators are able to read and write the management file that stores the challenge response used to unlock the system. The management file is protected by Windows.                        |
| CVE-2026-16438 | An arbitrary operation vulnerability due to Incorrect Privilege Assignment (CWE-266) <sup>4</sup> exists in GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, and MC Works64. During installation, the installers of the affected products unnecessarily grant default DCOM permissions to the administrator account of the affected products. As a result, users with that administrator accounts can locally or remotely launch and operate DCOM objects that should require UAC elevation. |

## Impact

If these vulnerabilities are exploited, they could result in information disclosure, tampering with, destruction, or deletion of information, and a denial-of-service (DoS) condition of the system.

| CVE ID         | Impact of the vulnerabilities                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2023-4863  | An attacker who has locally logged in to the PC may cause a heap-based buffer overflow and execute arbitrary code by importing a crafted file as an administrator for the affected product. As a result, the attacker may disclose internal information, tamper with, destroy, or delete internal information, or cause the affected system to enter a denial-of-service (DoS) condition. |
| CVE-2026-16436 | A remote attacker may be able to unlock the system by obtaining the challenge response by some means. As a result, the attacker may disclose internal information, tamper with, destroy, or delete internal information, or cause the affected system to enter a denial-of-service (DoS) condition.                                                                                       |
| CVE-2026-16437 | An attacker who has locally logged into the PC with administrator privileges may be able to unlock the system by tampering with the management file that stores the challenge response. As a result, the attacker may disclose internal information, tamper with, destroy, or delete internal information, or cause the affected system to enter a denial-of-service (DoS) condition.     |
| CVE-2026-16438 | An attacker who can log in using the same administrator account for the affected products may locally or remotely launch and operate DCOM objects. As a result, the attacker may disclose internal information, tamper with, destroy, or delete internal information, or cause the affected system to enter a denial-of-service (DoS) condition.                                          |

## Countermeasures for Customers

For customers using GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, and IoTWorX, please download and install the fixed version described in “Countermeasures for Products.” However, for customers who need to keep using the affected products, Mitsubishi Electric recommends to take the mitigations described in “Mitigations/Workarounds.”

For customers using MC Works64, Mitsubishi Electric recommends to take the mitigations described in “Mitigations/Workarounds” since there are no plans to release a fixed version. Alternatively, please consider replacing it with GENESIS64 or GENESIS. For information on how to replace it, please refer to the document below.

“GENESIS64 - How to replace MC Works64 with GENESIS64” (Japanese Only)

<sup>2</sup> <https://cwe.mitre.org/data/definitions/787.html>

<sup>3</sup> <https://cwe.mitre.org/data/definitions/640.html>

<sup>4</sup> <https://cwe.mitre.org/data/definitions/266.html>

Note: This document is published on our FA website, and membership registration and login are required to view it.

For customers using GENESIS32 and BizViz, Mitsubishi Electric recommends to take the mitigations described in "Mitigations/Workarounds" since there are no plans to release a fixed version. Alternatively, please consider replacing it with GENESIS64 or GENESIS.

## Countermeasures for Products

The following products have been fixed for these vulnerabilities.

| CVE ID                         | Affected products                                                  | Fixed version and how to get the installer                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2023-4863                  | GENESIS64 and ICONICS Suite                                        | It has been fixed in ICONICS Suite Version 10.97.3 or later<br><br>Please download and install from the link below.<br><a href="https://iconicsinc.my.site.com/community/s/resource-center/product-downloads">https://iconicsinc.my.site.com/community/s/resource-center/product-downloads</a><br>Note: GENESIS64 is included in the ICONICS Suite installation.                                          |
| CVE-2026-16436, CVE-2026-16437 | GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, and MobileHMI | It has been fixed in ICONICS Suite Version 10.98 or later<br><br>Please download and install from the link below.<br><a href="https://iconicsinc.my.site.com/community/s/resource-center/product-downloads">https://iconicsinc.my.site.com/community/s/resource-center/product-downloads</a><br>Note: GENESIS64, Hyper Historian, AnalytiX, and MobileHMI are included in the ICONICS Suite installation. |
|                                | IoTWorX                                                            | It has been fixed in IoTWorX 10.98 or later<br><br>Please download and install from the link below.<br><a href="https://hub.docker.com/r/iconics/iotworx">https://hub.docker.com/r/iconics/iotworx</a>                                                                                                                                                                                                    |
|                                | GENESIS                                                            | It has been fixed in GENESIS Version 11.04 or later<br><br>Please download and install from the link below.<br><a href="https://iconicsinc.my.site.com/community/s/resource-center/product-downloads">https://iconicsinc.my.site.com/community/s/resource-center/product-downloads</a>                                                                                                                    |
| CVE-2026-16438                 | GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, and MobileHMI | It has been fixed in ICONICS Suite Version 10.98 or later<br><br>Please download and install from the link below.<br><a href="https://iconicsinc.my.site.com/community/s/resource-center/product-downloads">https://iconicsinc.my.site.com/community/s/resource-center/product-downloads</a><br>Note: GENESIS64, Hyper Historian, AnalytiX, and MobileHMI are included in the ICONICS Suite installation. |

## Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting these vulnerabilities.

All vulnerabilities

- [1] 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, virtual private network (VPN), etc. and allow remote login only to administrator when internet access is required.
- [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.

CVE-2023-4863

- [1] Install anti-virus software on the PC with the affected product installed.

CVE-2026-16436 and CVE-2026-16437

- [1] Install anti-virus software on your PC with the affected product installed.
- [2] Perform the following steps for GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, and MC Works64.
  - 1) Delete the .dat file at the location specified below. This file name and location is different depending on the product version.  
Version 10: C:\Program Files\ICONICS\GENESIS64\Components\ClientChallengeTable.dat  
Version 11: C:\ProgramData\ICONICS\11\SecurityChallenges.dat
  - 2) Create a blank file with the same name and location.

- 3) Restrict the file system write and delete access to this file to a unique administrator account, different than the GENESIS administrator account.

CVE-2026-16438

- [1] Use the PCs with the affected product installed in the LAN and block access from untrusted networks and hosts through firewalls.
- [2] Block unauthorized access by using a firewall, virtual private network (VPN), etc. when internet access is required.
- [3] Install anti-virus software on the PC with the affected product installed, as well as on any PCs that can access it.

## Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>

<https://www.mitsubishielectric.com/fa/service-support/index.html>