

# Multiple Vulnerabilities in GENESIS64™ and MC Works64

Release date: November 28, 2024  
Mitsubishi Electric Corporation

## Overview

Multiple malicious code execution vulnerabilities exist in GENESIS64™ and MC Works64. An attacker may be able to execute a arbitrary code by storing a specially crafted DLL in a specific folder or tampering with a specially crafted DLL. This could lead to disclose information in the affected products, tamper with, destroy or delete information in the affected products, or cause a denial of service (DoS) condition on the products. (CVE-2024-8299, CVE-2024-8300, CVE-2024-9852).

For GENESIS64™ and MC Works64 versions prior to 10.97.3, they are unconditionally affected by CVE-2024-8299 and CVE-2024-9852. For versions 10.97.3 and later, they are affected if the multi-agent notification feature is installed. Additionally, if these products are installed in an unprotected folder other than the default installation folder, they are affected by CVE-2024-8300.

Affected versions of GENESIS64™ and MC Works64 are listed below. Please apply a security patch and take mitigations.

## CVSS<sup>2</sup>

CVE-2024-8299	CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Base Score: 7.8
CVE-2024-8300	CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Base Score: 7.0
CVE-2024-9852	CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Base Score: 7.8

## Affected products

<Affected products and versions>

CVE-2024-8299	: GENESIS64™ all versions and MC Works64 all versions
CVE-2024-8300	: GENESIS64™ Version 10.97.2, 10.97.2 CFR1, 10.97.2 CFR2, and 10.97.3
CVE-2024-9852	: GENESIS64™ all versions and MC Works64 all versions

<How to check your product version>

Open Windows® Control Panel and select "Programs and Features".

【If you are using MC Works64】

MC Works64 is applicable if the name is displayed as "MELSOFT MC Works64" and the version number is displayed as "10.95.210.01" or prior (Fig. 1).

Name	Publisher	Version
MELSOFT MC Works64	MITSUBISHI ELECTRIC CORPORATION	10.95.210.01

Figure 1 MC Works64 Version 4.04E (10.95.2)

【If you are using GENESIS64™ Version 10.97.2】

GENESIS64™ is applicable if the name is displayed as "ICONICS Suite" and the version number is displayed as "10.97.212.46" or prior (Fig. 2).

Name	Publisher	Version
ICONICS Suite	ICONICS	10.97.212.46

Figure 2 GENESIS64™ Version 10.97.2

If you are applying the Critical Fixes Rollup (CFR), please open the Windows® Settings menu, go to Apps > Installed Apps, and check the version of the installed CFR.

【If you are using GENESIS64™ Version 10.97.3】

GENESIS64™ is applicable if the name is displayed as "ICONICS Suite" and the version number is displayed as "10.97.306.55" (Fig. 3).

Name	Publisher	Version
ICONICS Suite	ICONICS	10.97.306.55

Figure 3 GENESIS64™ Version 10.97.3

<sup>2</sup> <https://www.first.org/cvss/v3.1/specification-document>

## Description

The following three vulnerabilities exist in GENESIS64™ and MC Works64.

- CVE-2024-8299 A malicious code execution vulnerability due to Uncontrolled Search Path Element (CWE-427<sup>2</sup>) exists in the Phone agent of the alarm multi-agent notification feature of GENESIS64™ and MC Works64. For GENESIS64™ and MC Works64 versions prior to 10.97.3, this vulnerability is unconditionally affected. For version 10.97.3 and later, they are affected if the multi-agent notification feature is installed.
- CVE-2024-8300 A malicious code execution vulnerability due to Dead Code(CWE-561<sup>3</sup>) exists in the FA device communication driver of GENESIS64™
- CVE-2024-9852 A malicious code execution vulnerability due to Uncontrolled Search Path Element (CWE-427) exists in the Phone agent of the alarm multi-agent notification feature on GENESIS64™ and MC Works64. For GENESIS64™ and MC Works64 versions prior to 10.97.3, this vulnerability is unconditionally affected. For version 10.97.3 and later, they are affected if the multi-agent notification feature is installed.

## Impact

An attacker may be able to execute a malicious code by storing a specially crafted DLL in a specific folder or tampering with a specially crafted DLL. This could lead to disclose information in the affected products, tamper with, destroy or delete information in the affected products, or cause a denial of service (DoS) condition on the products.

- CVE-2024-8299 An attacker may be able to execute a malicious code by storing a specially crafted DLL in a specific folder. This could lead to disclose information in the affected products, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.
- CVE-2024-8300 An attacker may be able to execute a malicious code by tampering with a specially crafted DLL. This could lead to disclose information in the affected products, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.
- CVE-2024-9852 An attacker may be able to execute a malicious code by storing a specially crafted DLL in a specific folder. This could lead to disclose information in the affected products, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.

## Countermeasures for Customers

Please apply a security patch listed in “Countermeasures for Products.” For CVE-2024-8299 and CVE-2024-9852, please take the mitigations described in "Mitigations / Workarounds" because there is no plans to release a fixed version.

## Countermeasures for Products

CVE-2024-8299 and CVE-2024-9852

There is no plans to release a fixed version.

CVE-2024-8300

The security patches corresponding to each version are as follows:

【If you are using GENESIS64™ Version 10.97.2 series】

”10.97.2 Critical Fixes Rollup 3”

(<https://iconicsinc.my.site.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-3>)

【If you are using GENESIS64™ Version 10.97.3 series】

”10.97.3 Critical Fixes Rollup 1”

(<https://iconicsinc.my.site.com/community/s/software-update/a35QQ000000y2oXYAQ/10973-critical-fixes-rollup-1>)

## Mitigations / Workarounds

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

All vulnerabilities

- 1) Use PCs with the affected product installed in the LAN and block remote login from untrusted networks, hosts, and users.
- 2) Prevent unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to trusted users when connecting a PC with the affected product installed to the Internet.
- 3) Restrict physical access to the PC on which the affected product is installed and the network to which the PC is connected to prevent unauthorized physical contact.
- 4) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

CVE-2024-8299 and CVE-2024-9852

If you do not need to use the multi-agent notification function, please uninstall it.

---

<sup>2</sup> <https://cwe.mitre.org/data/definitions/427.html>

<sup>3</sup> <https://cwe.mitre.org/data/definitions/561.html>

CVE-2024-8300

Do not install the affected products in non-default, unprotected folders.

## **Acknowledgement**

Mitsubishi Electric would like to thank Asher Davila and Malav Vyas, security researchers at Palo Alto Networks, who reported these vulnerabilities.

## **Contact information**

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>

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

## **Trademarks**

GENESIS64 is a trademark of ICONICS, Inc.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.