

# Arbitrary Code Execution and Information Disclosure vulnerabilities in AutoCAD (DWG) file import function of GENESIS64 and MC Works64

Release date: October 21, 2021  
Last update date: November 25, 2021  
Mitsubishi Electric Corporation

## ■ Overview

Arbitrary code execution vulnerability due to Out-of bounds Write (CVE-787) and information disclosure vulnerability due to Out-of bounds Read (CVE-125) exist in AutoCAD (DWG) file import function of GENESIS64 and MC Works64. An attacker may be able to execute arbitrary malicious code or disclose information by having target products import a specially crafted AutoCAD (DWG) file (CVE-2021-27040, CVE-2021-27041).

Versions of GENESIS64 and MC Works64 that are affected by these vulnerabilities are listed below, so please apply a security patch.

## ■ CVSS

CVE-2021-27040 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score:3.3  
CVE-2021-27041 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score:7.8

## ■ Affected products

<Affected products and their versions>

GENESIS64 : Version 10.97  
MC Works64 : Version 4.04E and prior

<How to check the version>

Open Windows® Control Panel and select “Programs and Features”.

GENESIS64 is applicable if the name is displayed as “ICONICS Suite” and the version number is displayed as “10.97.020.27” or prior (Fig. 1).

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. 2).

Name	Publisher	Version
ICONICS LanguagePack for 10.97	ICONICS	10.97.020.27
ICONICS Suite	ICONICS	10.97.020.27

Fig.1 GENESIS64

Name	Publisher	Version
MELSOFT Help	MITSUBISHI ELECTRIC CORPORATION	10.95.210.00
MELSOFT MC Works64	MITSUBISHI ELECTRIC CORPORATION	10.95.210.01
MELSOFT MCDemo	MITSUBISHI ELECTRIC CORPORATION	10.95.210.00

Fig.2 MC Works64

## ■ Description

Arbitrary code execution vulnerability (CVE-2021-27041) due to Out-of bounds Write (CVE-787) and information disclosure vulnerability (CVE-2021-27040) due to Out-of bounds Read (CVE-125) exist in AutoCAD (DWG) file import function of GENESIS64 and MC Works64.

## ■ Impact

An attacker may be able to execute arbitrary malicious code or disclose information by having target products import a specially crafted AutoCAD (DWG) file.

## ■ Countermeasures

Please update your software by using the GENESIS64 and MC Works64 security patches. The following are instructions for downloading the security patches.

### 1. Security patch for GENESIS64

Download the security patch from “SECURITY UPDATES” (<https://iconics.com/Support/CERT>) on ICONICS Web site.

- 1) For Users using GENESIS64 Version 10.97  
“10.97 Critical Fixes Rollup 2”

### 2. Security patch for MC Works64

Download the security patch from “MC Works64 AND MC Works32 SECURITY UPDATES”

(<https://iconics.com/Support/CERT-MC-Works>) on ICONICS Web site.

- 1) For Users using MC Works64 Version 4.04E  
“MC Works64 Version 4.04E (Version 10.95.210.01) Security Patches“
- 2) For Users using MC Works64 Edge-computing Edition Version 4.04E  
“MC Works64 Version 4.04E (Version 10.95.210.01) Security Patches“
- 3) For Users using MC Works64 Version 4.00A to 4.03D  
Please get the MC Works64 Version 4.04E installer from your local Mitsubishi Electric representative, install it, and then apply the security patch described in 2. 1).
- 4) For Users using MC Works64 Version 3.04E  
“MC Works64 Version 3.04E (Version 10.94.178.06) Security Patches“
- 5) For Users using MC Works64 Version 3.00A – 3.03D  
Please get the MC Works64 Version 3.04E installer from your local Mitsubishi Electric representative, install it, and then apply the security patch described in 2. 4).
- 6) For Users using MC Works64 Version 2.02C or earlier\*  
Please contact your local Mitsubishi Electric representative.

\* This applies if the version number is “10.87.148.42” or earlier in the version of “MELSOFT MC Works64”, which you can confirm in “How to check the version” of “Affected products”.

#### ■ Mitigations

Mitsubishi Electric recommends the following mitigation measures to minimize the risk of this vulnerability being exploited if the above countermeasures (applying security patches) cannot be implemented,

- (1) Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- (2) Restrict the connection of all control system devices and systems to the network so that they can only be accessed from trusted networks and hosts.
- (3) Avoid clicking on web links in emails etc. from untrusted sources. Also, avoid opening files attached to untrusted emails.

#### ■ Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>

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

#### ■ Update history

November 25, 2021

Added information about information disclosure vulnerability (CVE-2021-27040) due to Out-of bounds Read (CWE-125).