

Information Tampering Vulnerability in the project management function of GENESIS64™

Release date: December 13, 2022
Last update date: February 9, 2023
Mitsubishi Electric Corporation

■ Overview

An information tampering vulnerability due to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) exists in the project management function of GENESIS64™. Importing a project package file crafted by a malicious attacker may result in creating, tampering with or destroying arbitrary files. (CVE-2022-40264)

Versions of GENESIS64™ affected by this vulnerability are listed below, so please apply a security patch.

■ CVSS

CVE-2022-40264 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N Base Score: 6.3

■ Affected products

<Products and versions>

GENESIS64™ : Version 10.97 to 10.97.2

<How to check your product 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" to "10.97.212.46" (Fig. 1).


Name	Publisher	Version
 ICONICS Suite	ICONICS	10.97.212.46

Figure 1 An example of Windows® Control Panel

■ Description

An information tampering vulnerability due to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) exists in the project management function of GENESIS64™. (CVE-2022-40264)

■ Impact

Importing a project package file crafted by a malicious attacker may result in creating, tampering with or destroying arbitrary files.

■ Countermeasures

The GENESIS64™ security patches will be released soon. Please download security patches and update your software after the security patches are released.

1. Security patches for GENESIS64™

The security patch for GENESIS64™ can be downloaded from the ICONICS Community Portal (<https://iconics.force.com/community>), a web site operated by ICONICS. To download it, you need to create an account on this site and then enter a Support WorX Plan Number described in "SupportWorX License Information", which is shipped with the product.

- 1) For Users using GENESIS64™ Version 10.97.2
"10.97.2 Critical Fixes Rollup 1"
(<https://iconics.force.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-1>)
- 2) For Users using GENESIS64™ Version 10.97.1
Please take the mitigations described in "Mitigations/Workarounds". We are going to release the security patch for this version in the near future.
- 3) For Users using GENESIS64™ Version 10.97
Please take the mitigations described in "Mitigations/Workarounds". We are going to release the security patch for this version in the near future.

■ Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability if the above countermeasures (applying security patches) cannot be implemented.

- 1) Locate control system networks and devices behind firewalls and isolate them from untrusted networks and hosts.
- 2) Do not click on web links in e-mails from unreliable sources. Also, do not open attachments to untrusted e-mails.
- 3) Encrypt a project package file with a password to prevent modifications by untrustworthy users
- 4) Do not import a project package file if a relative path is found in the file contents. They are displayed on the screen when importing a file in the project management function.

■ 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.

■ Update history

February 9, 2023

Updated the release status of the security patch for GENESIS64™ Version 10.97.2, Version 10.97.1, Version 10.97

December 27, 2022

Updated the release status of the security patch for GENESIS64™ Version 10.97.2