

Malicious Code Execution Vulnerability in the Software Keyboard Function of GENESIS64, ICONICS Suite, Mobile HMI, and MC Works64

Release date: December 18, 2025
Mitsubishi Electric Corporation

Overview

Malicious code execution vulnerability exists in the software keyboard function (hereinafter referred to as “keypad function”) of GENESIS64, ICONICS Suite, MobileHMI, and MC Works64. An attacker may be able to execute arbitrary executable files (EXE) when a legitimate user uses the keypad function by tampering with the configuration file for the function (CVE-2025-11774). This could allow the attacker to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a denial-of-service (DoS) condition on the system, through the execution of the EXE.

Affected products and versions are listed below. Please follow the instructions in the “Countermeasures for Customers” section.

CVSS¹

CVE-2025-11774 CVSS:v3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H Base Score: 8.2

Affected products

<Affected products and versions>

GENESIS64 : Version 10.97.2 CFR3 and prior
ICONICS Suite : Version 10.97.2 CFR3 and prior
MobileHMI : Version 10.97.2 CFR3 and prior
MC Works64 : All versions

<How to check GENESIS64, ICONICS Suite, and MobileHMI version>

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

GENESIS64, ICONICS Suite, or MobileHMI will be displayed depending on the product and version installed. If the version shown is “10.97.212.46” or lower, it is applicable (Figure 1).


Name	Publisher	Version
 ICONICS Suite	ICONICS	10.97.212.46

Figure 1

Description

Malicious code execution vulnerability due to Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78²) exists in the keypad function of GENESIS64, ICONICS Suite, MobileHMI, and MC Works64.

Impact

An attacker may be able to execute arbitrary executable files (EXE) when a legitimate user uses the keypad function by tampering with the configuration file for the function. This could allow the attacker to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a denial-of-service (DoS) condition on the system, through the execution of the EXE .

Countermeasures for Customers

<Customers using MC Works64>

There is no plan to release a fixed version.

To minimize the risk of this vulnerability being exploited, please consider migrating to GENESIS64 v10.97.3 or later.

For instructions on how to perform the migration to GENESIS64, refer to the document below.

“GENESIS64 - How to replace MC Works64 with GENESIS64_JP” (Japanese Only)

(<https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf>)

<Customer using GENESIS64, ICONICS Suite, or MobileHMI>

This vulnerability has been fixed in GENESIS64 Version 10.97.3

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

² <https://cwe.mitre.org/data/definitions/78.html>

Please follow the steps in “Countermeasures for Products” to update to GENESIS64 Version 10.97.3 and apply the latest patch version, or upgrade to the latest product, GENESIS V11.

Countermeasures for Products

<MC Works64>

There are no plans to release a fixed version.

<GENESIS64, ICONICS Suite, or MobileHMI>

Version 10.97.3 can be downloaded by accessing Community Portal (<https://iconicsinc.my.site.com/community>) and navigating to “Resources > Product Downloads > 10.97.3.”

The latest patch version for GENESIS64 Version 10.97.3 can be downloaded from the link below:

<https://iconicsinc.my.site.com/community/s/software-update/a35QQ000000y2oXYAQ/10973-critical-fixes-rollup-2>

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability.

- 1) Use the PCs with the affected product installed in the LAN and block remote login from untrusted networks, hosts and users.
- 2) Block unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to trusted users, when connecting the PCs with the affected product installed to the Internet.
- 3) 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.
- 4) Do not click web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.
- 5) Install an antivirus software in the PC with the affected product installed.

Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>

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