Authentication Bypass Vulnerability in Web communication function on GENESIS64 and MC Works64

Release date: January 20, 2022
Mitsubishi Electric Corporation

■Overview

Authentication bypass vulnerability due to incomplete list of disallowed inputs (CWE-184) exists in GENESIS64 and MC Works64. An attacker may bypass the authentication of GENESIS64 and MC Works64 by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of GENESIS64 and MC Works64, and gain unauthorized access to GENESIS64 and MC Works64.（CVE-2022-23128）

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

■CVSS

CVE-2022-23128 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:9.8

■Affected products

<Affected products and their versions>

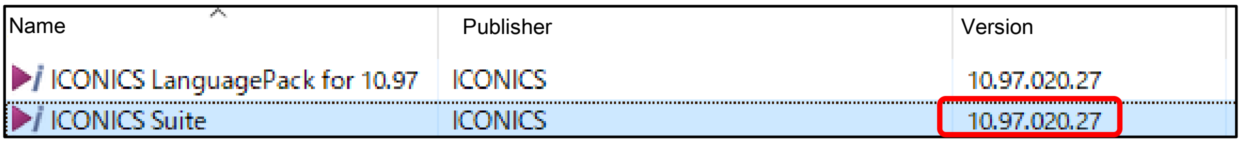
GENESIS64	: Version 10.97
MC Works64	: Version 4.00A to 4.04E

<How to check the version>

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

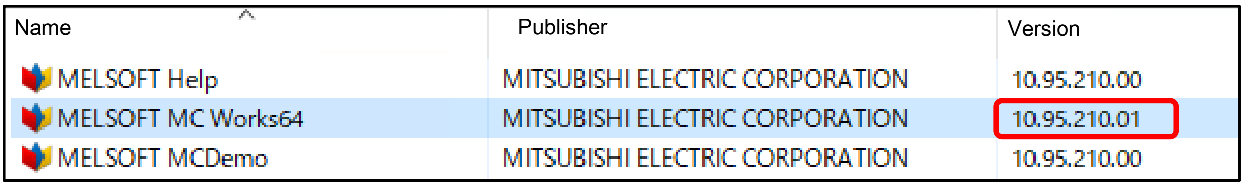
GENESIS64 is applicable if the name displays ″ICONICS Suite″ and the version number displays ″10.97.020.27″ or prior (Fig. 1).

MC Works64 is applicable if the name is displayed as ″MELSOFT MC Works64″ and the version number is displayed as “10.95.201.23” to ″10.95.210.01″ (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

Authentication bypass vulnerability due to incomplete list of disallowed inputs (CWE-184) exists in GENESIS64 and MC Works64.

■Impact

An attacker may bypass the authentication of GENESIS64 and MC Works64 by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of GENESIS64 and MC Works64, and gain unauthorized access to GENESIS64 and MC Works64.（CVE-2022-23128）

■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

   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 the patch, you need to create an account for free on this site and assign a Support WorX Plan Number as shown in “SupportWorX License Information” included with the product to the account.

   1) For Users using GENESIS64 Version 10.97
      “10.97 Critical Fixes Rollup 2”
      (https://iconics.force.com/community/s/software-update/a355a00000304zLAAS/1097-critical-fixes-rollup-2-including-language-pack-and-devicexplorer-640)

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).

＊This applies if the version number is from ″10.95.201.23″ to ″10.95.209.08″ 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) Switch the communication method of FrameWorX server from WebSocket communication to WCF communication. Set “WebSocketTransport” element to “false” in ″FwxServer.Network.config″ file located in the installation folder of the products.
(2) Locate control system networks and remote devices behind firewalls and isolate them from the business network.
(3) 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.

■Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>
https://www.mitsubishielectric.com/fa/support/index.html