Information Disclosure, Information Tampering and Denial of Service (DoS) Vulnerability in GENESIS64^{TM} and MC Works64

Release date: October 22, 2024
Mitsubishi Electric Corporation

Overview

Information disclosure, information tampering and denial of service (DoS) vulnerability due to incorrect permission settings on a folder during installation exists in GenBroker32, which is included in the installers for GENESIS64^{TM} and MC Works64, when GenBroker32 is installed on the same PC as GENESIS64^{TM} or MC Works64. A malicious local authenticated attacker may be able to disclose or tamper with confidential information and data contained in the products, or cause a denial of service (DoS) condition on the products, by accessing a folder with incorrect permissions. (CVE-2024-7587)

The versions of GENESIS64^{TM} and MC Works64 including the affected GenBroker32 installer are listed below. Please apply the countermeasures, workarounds, or mitigations.

CVSS[1]

CVE-2024-7587 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

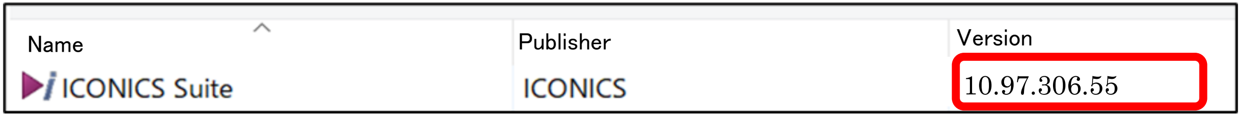
<Affected products and versions>

GENESIS64^{TM} Version 10.97.3 and prior
MC Works64 All versions

<How to check your product version>

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

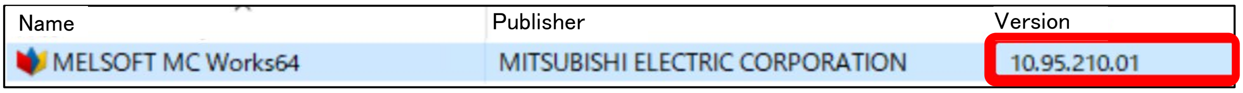
GENESIS64^{TM} is applicable if the name is displayed as "ICONICS Suite" and the version number is displayed as "10.97.306.55" or prior (Fig. 1).



Name	Publisher	Version
ICONICS Suite	ICONICS	10.97.306.55

Figure 1 GENESIS64^{TM} Version 10.97.3

MC Works64 is applicable if the name is displayed as "MELSOFT MC Works64" and the version number is displayed as "10.97.201.01" or prior (Fig. 2).



Name	Publisher	Version
MELSOFT MC Works64	MITSUBISHI ELECTRIC CORPORATION	10.95.210.01

Figure 2 MC Works64 Version 4.04E

Description

Information disclosure, information tampering and denial of service (DoS) vulnerability due to Incorrect Default Permissions (CWE-276[2]) exists in GenBroker32, when GenBroker32 is installed on the same PC as GENESIS64^{TM} or MC Works64.

Impact

A malicious local authenticated attacker may be able to disclose or tamper with confidential information and data stored in C:\ProgramData\ICONICS folder, or cause a denial of service (DoS) condition on the products, by accessing the folder with incorrect permissions.

Countermeasures

<Customer using GENESIS64^{TM} Version 10.97.3>

Please uninstall GenBroker32, apply the security patch to GENESIS64^{TM} and then reinstall GenBroker32. The security patch 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 SupportWorX Plan Number described in "SupportWorX License Information", which is shipped with the product.

<Cutomers using GENESIS64^{TM} Version 10.97.2 or prior including MC Works64>

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/276.html

Please upgrade your product to GENESIS64^{TM} Version 10.97.3 and reinstall GenBroker32 following the instructions above. If you have difficulty upgrading your product, please apply workarounds and mitigations.

Workarounds

Manually remove "Everyone" from the folder permissions for the C:\ProgramData\ICONICS folder on the PC where GenBroker32 is installed and all folders under it. If you would like to remove the permission recursively including subfolders, please follow the following steps.

1. Right click C:\ProgramData\ICONICS folder and open the Properties display
2. Open the Security tab
3. Click Advanced
4. Click Change Permissions
5. Select “Everyone” and check the “Replace all object permissions entries with inheritable permission entires from this project” checkbox
6. Click Remove

Mitigations

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

1) Use PC with the affected product installed within a LAN to block remote login from untrusted networks, hosts, and users.
2) When PC with the affected product installed are connected to the Internet, prevent unauthorized access by using firewalls, virtual private networks (VPN), etc., and allow remote login only to trusted users.
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 contact.
4) Install anti-virus software on the PC on which the affected product is used, and prevent the user from clicking on web links in e-mails or other messages from untrusted sources, or from opening attachments in untrusted e-mails.

Acknowledgement

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

Contact information

Please contact your local Mitsubishi Electric representative.

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