Multiple Vulnerabilities in GENESIS64™ and MC Works64

Release date: July 19, 2022
Last update date: August 3, 2023
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities exist in GENESIS64™ and MC Works64. Exploiting these vulnerabilities by a malicious attacker may result in information disclosure, Denial of Service (DoS) condition or remote code execution. (CVE-2022-29834, CVE-2022-33315, CVE-2022-33316, CVE-2022-33317, CVE-2022-33318, CVE-2022-33319, CVE-2022-33320)
Versions of GENESIS64™ and MC Works64 that are affected by these vulnerabilities are listed below, so please apply a security patch.

■CVSS

CVE-2022-29834 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 7.5
CVE-2022-33315 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score: 7.8
CVE-2022-33316 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score: 7.8
CVE-2022-33317 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score: 7.8
CVE-2022-33318 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score: 9.8
CVE-2022-33319 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H Base Score: 8.2
CVE-2022-33320 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

<Products and versions>

GENESIS64™ : Version 10.97 to 10.97.1
MC Works64 : Version 4.04E and prior (excluding CVE-2022-29834)

<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 "10.97.112.56" 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).

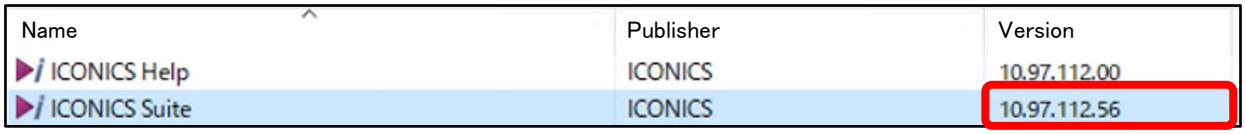

Figure 1 GENESIS64™

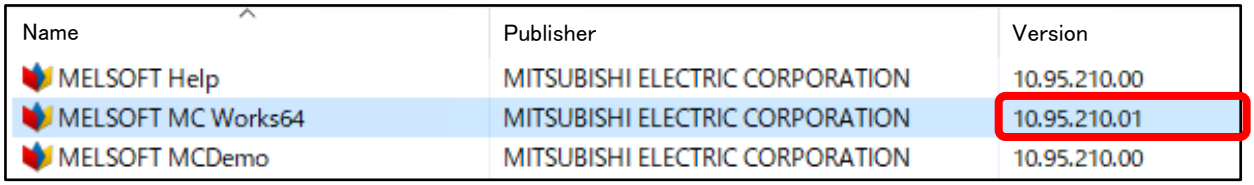

Figure 2 MC Works64

■Description

The following seven vulnerabilities exist in GENESIS64™ and MC Works64.

CVE-2022-29834 An information disclosure vulnerability via Path Traversal (CWE-22) exists in the mobile monitoring function of GENESIS64™ due to an improper input validation for URL parameters.
CVE-2022-33315 A remote code execution vulnerability resulting from Deserialization of Untrusted Data (CWE-502) exists in the graphic monitoring function of GENESIS64™ and MC Works64 due to an improper input validation for monitoring screen files.
CVE-2022-33316 A remote code execution vulnerability resulting from Deserialization of Untrusted Data (CWE-502) exists in the graphic monitoring function of GENESIS64™ and MC Works64 due to an improper input validation for monitoring screen files.
CVE-2022-33317 A remote code execution vulnerability via Inclusion of Functionality from Untrusted Control Sphere (CWE-829) exists in the graphic monitoring function of GENESIS64™ and MC Works64 due to improper restriction of scripting.

CVE-2022-33318 A remote code execution vulnerability resulting from Deserialization of Untrusted Data (CWE-502) exists in the communication function of GENESIS64™ and MC Works64 with an external OPC DA server due to an improper input validation for packets.

CVE-2022-33319 An information disclosure and Denial of Service (DoS) vulnerability resulting from Out-of-bounds Read (CWE-125) exists in the communication function of GENESIS64™ and MC Works64 with an external OPC DA server due to improper input data size validation for packets.

CVE-2022-33320 A remote code execution vulnerability resulting from Deserialization of Untrusted Data (CWE-502) exists in the project management function of GENESIS64™ and MC Works64 due to an improper input validation for project configuration files.

■Impact

Exploiting these vulnerabilities by a malicious attacker may results in information disclosure of the product, Denial of Service (DoS) condition of the product or a remote code execution.

CVE-2022-29834 An attacker may be able to access to arbitrary files in the GENESIS64™ server and disclose information stored in the files by embedding a malicious URL parameter in the URL of the monitoring screen delivered to the GENESIS 64™ mobile monitoring application and access the monitoring screen.

CVE-2022-33315 An attacker may be able to execute an arbitrary malicious code by leading a user to load a monitoring screen file including malicious XAML codes.

CVE-2022-33316 An attacker may be able to execute an arbitrary malicious code by leading a user to load a monitoring screen file including malicious XAML codes.

CVE-2022-33317 An attacker may be able to execute an arbitrary malicious code by leading a user to load a monitoring scree file including malicious script codes.

CVE-2022-33318 An attacker may be able to execute an arbitrary malicious code by sending specially crafted packets to the GENESIS64™ server.

CVE-2022-33319 An attacker may be able to disclose information on memory or cause a Denial of Service (DoS) condition by sending specially crafted packets to the GENESIS64™ server.

CVE-2022-33320 An attacker may be able to execute an arbitrary malicious code by leading a user to load a project configuration file including malicious XML codes.

■Countermeasures

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

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 10.97.1
"10.97.1 Critical Fixes Rollup 3"
(https://iconics.force.com/community/s/software-update/a355a000003WwejAAC/10971-critical-fixes-rollup-3)

2) For Users using GENESIS64™ Version 10.97
"10.97 Critical Fixes Rollup 4"
(https://iconicsinc.my.site.com/community/s/software-update/a355a000003O4zLAAS/1097-critical-fixes-rollup-4)

2. Security patches 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
Please take the mitigations described in "Mitigations/Workarounds". We are currently developing a security patch for this version and going to release it in the near future.

2) For Users using MC Works64 Version Edge-computing Edition Version 4.04E
Please take the mitigations described in "Mitigations/Workarounds". We are currently developing a security patch for this version and going to release it in the near future.

3) For Users using MC Works64 Version 4.00A to 4.03D*1
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).

*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".

4) For Users using MC Works64 Version 3.04E or prior*2
Please contact your local Mitsubishi Electric representative.
*2 This applies if the version number is "10.94.178.06" or prior in the version of "MELSOFT MC Works64", which you can confirm in "How to check the version" of "Affected products".

■Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting these vulnerabilities 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.

■Contact information

Please contact your local Mitsubishi Electric representative.

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

■Update history

August 3, 2023
Added the security patch information for GENESIS64™ Version 10.97 in "Countermeasures"

February 9, 2023
Updated the release date of security patches for GENESIS64™ Version 10.97, MC Works64 Version 4.04E and MC Works64 Edge-computing Edition Version 4.04E

December 15, 2022
Updated the release date of security patches for GENESIS64™ Version 10.97, MC Works64 Version 4.04E and MC Works64 Edge-computing Edition Version 4.04E

September 30, 2022
Updated the release date of security patches for GENESIS64™ Version 10.97, MC Works64 Version 4.04E and MC Works64 Edge-computing Edition Version 4.04E

August 30, 2022
Added the security patch information for GENESIS64™ Version 10.97.1 in "Countermeasures"