Denial of Service (DoS) Vulnerability in OPC UA communication function of GENESIS64 and MC Works64

Release date: October 21, 2021
Mitsubishi Electric Corporation

■Overview

Denial of Service (DoS) vulnerability exists in OPC UA SDK installed in GENESIS64 and MC Works64. A remote attacker may be able to cause a denial of service condition by sending a specially crafted packet (CVE-2021-27432).
Versions of GENESIS64 and MC Works64 that are affected by this vulnerability are listed below, so please apply a security patch.

■CVSS

CVE-2021-27432 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

<Affected products and their versions>

GENESIS64 : Version 10.97
MC Works64 : Version 4.04E and prior

<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 "10.95.210.01" or prior (Fig. 2).

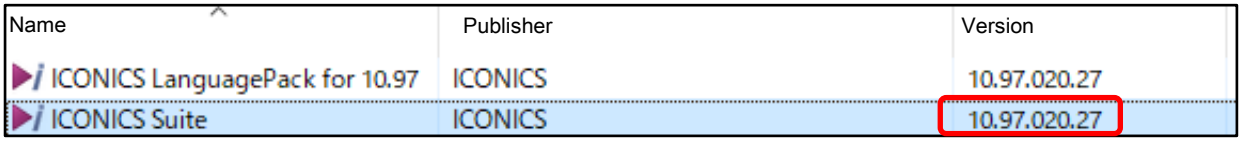

Fig.1 GENESIS64

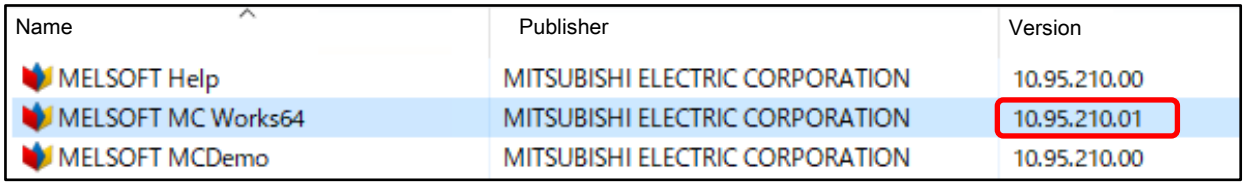

Fig.2 MC Works64

■Description

Denial of Service (DoS) vulnerability due to uncontrolled recursion (CWE-674) exists in a OPC UA communication function of GENESIS64 and MC Works64.

■Impact

A remote attacker can cause a denial of service condition by sending a specially crafted OPC UA packet.

■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
   Download the security patch from "SECURITY UPDATES" (https://iconics.com/Support/CERT) on ICONICS Web site.

   1) For Users using GENESIS64 Version 10.97
      "10.97 Critical Fixes Rollup 2"

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).

4) For Users using MC Works64 Version 3.04E
“MC Works64 Version 3.04E (Version 10.94.178.06) Security Patches“

5) For Users using MC Works64 Version 3.00A – 3.03D
Please get the MC Works64 Version 3.04E installer from your local Mitsubishi Electric representative, install it, and then apply the security patch described in 2. 4).

6) For Users using MC Works64 Version 2.02C or earlier*
Please contact your local Mitsubishi Electric representative.

* This applies if the version number is ″10.87.148.42″ or earlier 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) Locate control system networks and remote devices behind firewalls and isolate them from the business network.
(2) 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.
(3) Use the security certificate of OPC UA so that GENESIS64 and MC Works64 can connect only with trusted OPC UA servers and clients.

■Contact information

Please contact your local Mitsubishi Electric representative.

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