Denial-of-Service (DoS) and Remote Code Execution Vulnerabilities in the BACnet® secure connect function of GENESIS64™

Release date: March 7, 2023
Last update date: August 30, 2023
Mitsubishi Electric Corporation

■Overview

Multiple Denial-of-Service (DoS) and Remote Code Execution vulnerabilities due to Buffer Copy without Checking Size of Input (CWE-120) exist in the OpenSSL library which is installed in GENESIS64™. Importing a X.509 digital certificate crafted by a malicious attacker into the BACnet® secure connect function using the affected OpenSSL library may cause denial of service (DoS) condition (CVE-2022-3602, CVE-2022-3786) or remote code execution (CVE-2022-3602). Note that this function is installed on GENESIS64™ as a beta version and it is disabled by the default configuration. These vulnerabilities do not affect unless the function is enabled explicitly.

Versions of GENESIS64™ affected by these vulnerabilities are listed below, so please apply a security patch.

■CVSS

CVE-2022-3602 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score: 8.1
CVE-2022-3786 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score: 5.9

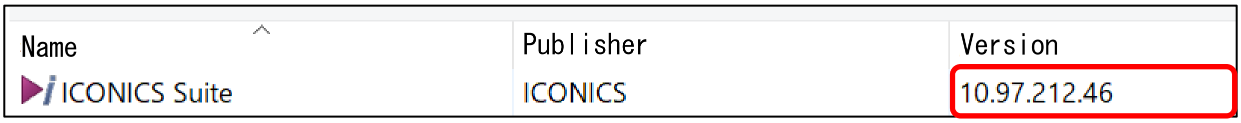
■Affected products

<Affected products and versions>

GENESIS64™ : Version 10.97.2

<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 "10.97.212.46" (Fig. 1).



Name	Publisher	Version
ICONICS Suite	ICONICS	10.97.212.46

Figure 1 An example of Windows® Control Panel

■Description

Multiple Denial-of-Service (DoS) and Remote Code Execution vulnerabilities due to Buffer Copy without Checking Size of Input (CWE-120) caused by the improper verification of X.509 digital certificate exist in the OpenSSL library which is installed in GENESIS64™.

■Impact

Importing a X.509 digital certificate crafted by a malicious attacker into the BACnet® secure connect function using the affected OpenSSL library may cause denial of service (DoS) condition or remote code execution. Note that this function is installed on GENESIS64™ as a beta version and it is disabled by the default configuration. These vulnerabilities do not affect unless the function is enabled explicitly.

■Countermeasures

Please update your software by using the GENESIS64™ security patch. It 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.

- "10.97.2 Critical Fixes Rollup 1"
  (https://iconics.force.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-1)

■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) Disable the BACnet® secure connect function if it is enabled. Note that this function is installed on GENESIS64™ as the beta version and it is disabled by the default configuration. Please refer to [Home > Common Tools > Data Connectivity > BACnet/SC > Overview of BACnet/SC > Using BACnet with the SC Point Manager] in ICONICS

Pruduct Help (https://docs.iconics.com/V10.97.2/GENESIS64/Help/ICONICS_Product_Help.htm#Com/Intro/ICONICS_Product_Help.htm) for the procedure to disable this function.

2) Locate control system networks and devices behind firewalls and isolate them from untrusted networks and hosts.

3) Physically protect the BACnet® network in the control system to prevent untrusted devices from connecting to the system.

■Contact information

Please contact your local Mitsubishi Electric representative.

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

■Trademarks

BACnet is a registered trademark of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
GENESIS64 is a trademark of ICONICS, Inc.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

■Update history

August 30, 2023

Added information of Remote Code Execution vulnerability (CVE-2022-3602) due to Buffer Copy without Checking Size of Input (CWE-120). Also changed the title of this advisory.