

Multiple Vulnerabilities in GENESIS64™ and MC Works64

Release date: June 27, 2024
Update date: October 17, 2024
Mitsubishi Electric Corporation

Overview

Multiple vulnerabilities exist in GENESIS64™ and MC Works64. These vulnerabilities may allow a malicious attacker to cause Denial of Service (DoS) condition, execute malicious code, or bypass authentication. (CVE-2023-2650, CVE-2023-4807, CVE-2024-1182, CVE-2024-1573, CVE-2024-1574)

Affected versions of GENESIS64™ and MC Works64 are listed below. Please apply a security fix or take mitigations.

CVSS¹

CVE-2023-2650	CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L	Base Score: 3.7
CVE-2023-4807	CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 5.9
CVE-2024-1182	CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Base Score: 7.0
CVE-2024-1573	CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	Base Score: 5.9
CVE-2024-1574	CVSS:v3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Base Score: 6.7

Affected products

<Affected products and versions>

CVE-2023-2650	: GENESIS64™ Version 10.97.2
CVE-2023-4807	: GENESIS64™ Version 10.97.2
CVE-2024-1182	: GENESIS64™ all versions and MC Works64 all versions
CVE-2024-1573	: GENESIS64™ Versions 10.97 to 10.97.2 and MC Works64 all versions
CVE-2024-1574	: GENESIS64™ Versions 10.97 to 10.97.2 and MC Works64 all versions

<How to check your product version>

CVE-2023-2650 and CVE-2023-4807

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).

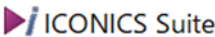
Name	Publisher	Version
	ICONICS	10.97.212.46

Figure 1 GENESIS64™ Version 10.97.2

CVE-2024-1182

GENESIS64™ all versions and MC Works64 all versions are affected.

CVE-2024-1573 and CVE-2024-1574

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" or prior (Fig. 1).

MC Works64 all versions are affected.

Description

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

- CVE-2023-2650 When the BACnet® Secure Connect feature is enabled in GENESIS64™, a Denial of Service (DoS) vulnerability due to Allocation of Resources Without Limits or Throttling (CWE-770²) exists in the OpenSSL library integrated into the products, during data validation. Note that the BACnet® Secure Connect feature is installed in the affected versions as a beta version and is disabled by default. The vulnerability is not threatened unless this feature is explicitly enabled.
- CVE-2023-4807 When running on X86_64 CPUs supporting AVX512-IFMA instructions and the BACnet® Secure Connect feature is enabled in GENESIS64™, a Denial of Service (DoS) vulnerability due to Improper Verification of Cryptographic Signature (CWE-347³) exists in the Message Authentication Code (MAC) implementation in OpenSSL library integrated into the products. Note that the BACnet® Secure Connect feature is installed in the

¹ <https://www.first.org/cvss/v3.1/specification-document>

² <https://cwe.mitre.org/data/definitions/770.html>

³ <https://cwe.mitre.org/data/definitions/347.html>

- affected versions as a beta version and is disabled by default. The vulnerability is not threatened unless this feature is explicitly enabled.
- CVE-2024-1182 When GENESIS64™ and MC Works64 are installed with the Pager agent in the alarm multi-agent notification feature, a malicious code execution vulnerability due to Uncontrolled Search Path Element (CWE-427⁴) exists in the feature.
- CVE-2024-1573 An authentication bypass vulnerability due to Improper Authentication (CWE-287⁵) exists in the mobile monitoring feature of GENESIS64™ and MC Works64 when all of the following conditions are met:
- Active Directory is used in the security setting.
 - "Automatic log in" option is enabled in the security setting.
 - The IcoAnyGlass IIS Application Pool is running under an Active Directory Domain Account.
 - The IcoAnyGlass IIS Application Pool account is included in GENESIS64™ and MC Works64 Security and has permission to log in.
- CVE-2024-1574 A malicious code execution vulnerability due to Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (CWE-470⁶) exists in the licensing feature of GENESIS64™ and MC Works64.

Impact

- CVE-2023-2650 The BACnet® Secure Connect feature using the affected library may temporarily cause a Denial of Service (DoS) condition when receiving and verifying a certificate that contains a specially crafted ASN.1 OBJECT IDENTIFIER.
- CVE-2023-4807 The BACnet® Secure Connect feature using the affected library may cause a Denial of Service (DoS) condition when receiving and processing messages that contains specially crafted Message Authentication Codes (MAC).
- CVE-2024-1182 An attacker may be able to execute malicious code by storing a specially crafted DLL in a specific folder.
- CVE-2024-1573 A malicious unauthenticated attacker may bypass proper authentication and log in to the system.
- CVE-2024-1574 An attacker may be able to execute malicious code with administrative privileges by tampering with a specific file that is not protected by the system.

Countermeasures

CVE-2023-2650

Please update your software by using the GENESIS64™ security fix. 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 SupportWorX Plan Number described in "SupportWorX License Information", which is shipped with the product.

"10.97.2 Critical Fixes Rollup 3"

(<https://iconicsinc.my.site.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-3>)

CVE-2023-4807

A security fix applicable to affected versions is currently under development, and will be released when it is ready. Until the security fix is released, please take the mitigations described in "Mitigations/Workarounds."

CVE-2024-1182

Please take the mitigations described in "Mitigations/Workarounds" since there is no plans to release a fix version.

CVE-2024-1573 and CVE-2024-1574

GENESIS64™ Version 10.97.3 and later is not vulnerable to this vulnerability. Please consider to upgrade the GENESIS64™ version to remove the threats caused by this vulnerability.

For users who need to keep using the affected version of GENESIS64™ and MC Works64, Mitsubishi Electric strongly recommends to take the mitigations and workarounds as described below.

Mitigations / Workarounds

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

All vulnerabilities

- 1) Locate control system networks and devices behind firewalls and isolate them from untrusted networks and hosts.
- 2) Restrict physical access to the personal computer where the product is installed and the network to which the personal computer is connected to prevent unauthorized contact.
- 3) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

⁴ <https://cwe.mitre.org/data/definitions/427.html>

⁵ <https://cwe.mitre.org/data/definitions/287.html>

⁶ <https://cwe.mitre.org/data/definitions/470.html>

CVE-2023-2650

- 1) Disable the BACnet® Secure Connect feature 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 ICONICS Product Help (https://docs.iconics.com/V10.97.2/GENESIS64/Help/Apps/WBDT/BACnet_SC/Overview_of_BACnet_SC.htm) for the procedure to disable this function.
- 2) Avoid importing certificates from untrusted sources.

CVE-2023-4807

- 1) Disable the BACnet® Secure Connect feature 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 ICONICS Product Help (https://docs.iconics.com/V10.97.2/GENESIS64/Help/Apps/WBDT/BACnet_SC/Overview_of_BACnet_SC.htm) for the procedure to disable this function.

CVE-2024-1182

- 1) The affected feature, the alarm multi-agent notification feature, is no longer the part of the default installation for GENESIS64™ Version 10.97.3 and later. Please do not custom install this feature unless you specifically need it.

CVE-2024-1573

- 1) In the security settings of GENESIS64™ and MC Works64, ensure that at least one of the following four conditions is not met.
 - Active Directory is used in the security setting.
 - “Automatic log in” option is enabled in the security setting.
 - The IcoAnyGlass IIS application pool is running under an Active Directory Domain Account.
 - The IcoAnyGlass IIS Application Pool account is included in GENESIS64™ and MC Works64 Security and has permission to log in.

Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>

<https://www.mitsubishielectric.com/fa/support/index.html>

Acknowledgement

Mitsubishi Electric would like to thank Asher Davila and Malav Vyas, security researchers at Palo Alto Networks, who reported CVE-2024-1182.

Trademarks

GENESIS64 is a trademark of ICONICS, Inc.

BACnet is a registered trademark of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Update history

October 17, 2024

Added the Acknowledgement.