Multiple Vulnerabilities due to OpenSSL Vulnerabilities in the BACnet® secure connect function of GENESIS64™

Release date: August 17, 2023
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities exist in OpenSSL library which is installed in GENESIS64™. These vulnerabilities could allow a remote attacker to disclose information or cause Denial of Service (DoS) condition (CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0401). 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™ that are affected by these vulnerabilities are listed below, so please apply a security patch.

■CVSS[1]

CVE-2022-4203	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H	Base Score: 4.4
CVE-2022-4304	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score: 5.9
CVE-2022-4450	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 5.9
CVE-2023-0401	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 5.9

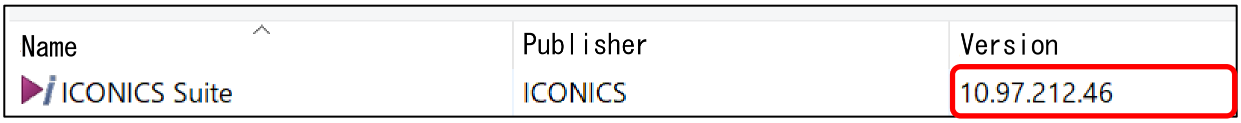
■Affected products

<Affected products and versions>

GENESIS64™ : Version 10.97.2

<How to check your product version>

Open Windows® Control Panel and select "Programs" and then "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

The following four vulnerabilities exist in GENESIS64™.

CVE-2022-4203 A denial of service (DoS) vulnerability exists in the OpenSSL library in GENESIS64™ due to Out-of-bounds Read (CWE-125[2]) triggered in X.509 certificate verification, specifically in name constraint checking.

CVE-2022-4304 An information disclosure vulnerability exists in the OpenSSL library in GENESIS64™ due to Observable Timing Discrepancy (CWE-208[3]) in RSA decryption implementations.

CVE-2022-4450 A denial of service (DoS) vulnerability exists in the OpenSSL library in GENESIS64™ due to Double Free (CWE-415[4]) when reading a PEM file.

CVE-2023-0401 A denial of service (DoS) vulnerability exists in the OpenSSL library in GENESIS64™ due to NULL Pointer Dereference (CWE-476[5]) while signatures are being verified.

■Impact

These vulnerabilities could allow a remote attacker to disclose information or cause Denial of Service (DoS) condition on the product. Note that BACnet® secure connect function is installed on GENESIS64™ as the beta version and it is disabled by the default configuration. These vulnerabilities do not cause threats unless a user explicitly activates this function.

CVE-2022-4203 An attacker may be able to cause a denial of service (DoS) by leading a user who uses the BACnet® secure connect function with the affected library to validate a malicious X.509 certificate.

CVE-2022-4304 An attacker may be able to disclose information by decrypting ciphertext in a Bleichenbacher style attack[*1].

[1] https://www.first.org/cvss/v3.1/specification-document
[2] https://cwe.mitre.org/data/definitions/125.html
[3] https://cwe.mitre.org/data/definitions/208.html
[4] https://cwe.mitre.org/data/definitions/415.html
[5] https://cwe.mitre.org/data/definitions/476.html

CVE-2022-4450 An attacker may be able to cause a denial of service (DoS) by leading a user who uses the BACnet® secure connect function with the affected library to read a malicious PEM file (public key or certificate).

CVE-2023-0401 An attacker may be able to cause a denial of service (DoS) by leading a user who uses the BACnet® secure connect function with the affected library to verify signatures when the FIPS mode is enabled.

*[1] An attack method to decrypt ciphertext by observing the behavior when a padding error occurs

■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 SupportWorX Plan Number described in "SupportWorX License Information", which is shipped with the product.

- "10.97.2 Critical Fixes Rollup 2"
(https://iconicsinc.my.site.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-2)

■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 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) 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

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.