Multiple Information Disclosure, Tampering, and Denial-of-Service Vulnerabilities in GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, MC Works64, and GENESIS

Release date: April 7, 2026
Mitsubishi Electric Corporation

Overview

Multiple information disclosure, tampering, and Denial-of-Service (DoS) vulnerabilities exist in GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, MC Works64, and GENESIS. When the local cache (SQLite) feature of affected products is enabled and the SQL Server authentication method is SQL authentication, an attacker may be able to disclose SQL Server credentials stored on the PC where the product is installed (CVE-2025-14815). And, when the SQL Server authentication method is SQL authentication, an attacker may be able to disclose SQL Server credentials from the screen of affected products (CVE-2025-14816). As a result, the attacker could access the SQL Server illegally to disclose data, tamper with or destroy data, and cause a denial-of-service (DoS) condition on the system.

The versions of products affected by these vulnerabilities are listed below. Please implement the measures described in the "Countermeasures for Customers" section.

CVSS[1]

CVE-2025-14815	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	Base Score:9.3
CVE-2025-14816	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	Base Score:9.3

Affected products

<Affected products and versions>

GENESIS64	: Version 10.97.3 and prior
ICONICS Suite	: Version 10.97.3 and prior
MobileHMI	: Version 10.97.3 and prior
Hyper Historian	: Version 10.97.3 and prior
AnalytiX	: Version 10.97.3 and prior
MC Works64	: All versions
GENESIS	: Version 11.02 and prior

<How to check GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX>
Open the Control Panel and select Programs > Programs & Features.
It is applicable if the version displayed for the affected product* is "10.97.305.55" or prior (Figure. 1).
*Versions 10.96.2 or later of GENESIS64, MobileHMI, Hyper Historian, and AnalytiX are bundled in the installation, so the product name appears as "ICONICS Suite".

Figure 1 GENESIS Version 10.97.3

<How to check GENESIS>
Open the Control Panel and select Programs > Programs & Features.
It is applicable if the version displayed in "ICONICS GENESIS" is "11.2.394" or prior. (Figure. 1).

Figure 1 GENESIS Version11.02

Description

There are two vulnerabilities in GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, MC Works64 and GENESIS.

CVE-2025-14815 When the local caching feature using SQLite is enabled and SQL authentication is used for the SQL Server authentication, the SQL Server credentials are stored in plaintext within the local SQLite file. This results in a vulnerability due to Cleartext Storage of Sensitive Information (CWE-312[2]), which may lead to information

1 https://www.first.org/cvss/v4-0/specification-document
2 https://cwe.mitre.org/data/definitions/312.html

disclosure, tampering, or denial-of-service (DoS).

CVE-2025-14816 In the Hyper Historian Splitter feature of the affected products, when SQL authentication is used for the SQL Server authentication, the SQL Server credentials are displayed in plain text in the GUI. This results in a vulnerability due to Cleartext Storage of Sensitive Information in GUI (CWE-317[3]), which may lead to information disclosure, tampering, or denial-of-service (DoS).

Impact

An attacker may be able to disclose the SQL Server credentials used by the affected products by exploiting these vulnerabilities. As a result, the unauthorized attacker could access the SQL Server and disclose, tamper with, or destroy data on the server, potentially cause a denial-of-service (DoS) condition on the system.

Countermeasures for Customers

CVE-2025-14815

<Customers using GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX>

Please download and install the latest product described in “Countermeasures for Products.”

After installation, perform the mitigations described for “CVE-2025-14815” under “Mitigations / Workarounds.”

<Customers using MC Works64>

There are no plans to release a fixed version, so please take the mitigations described in "Mitigations/Workarounds."

To minimize the risk of this vulnerability being exploited, please consider replacing it with GENESIS64. For information on how to replace it, please refer to the document below.

“GENESIS64 - How to replace MC Works64 with GENESIS64” (Japanese Only)
(https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf)

<Customers using GENESIS>

Please download and install the latest product described in “Countermeasures for Products.”

After installation, perform the mitigations described for “CVE-2025-14815” under “Mitigations / Workarounds.”

CVE-2025-14816

<Customers using GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX>

Please download and install the latest product described in “Countermeasures for Products.”

<Customers using MC Works64>

There are no plans to release a fixed version, so please take the mitigations described in "Mitigations/Workarounds."

To minimize the risk of this vulnerability being exploited, please consider replacing it with GENESIS64. For information on how to replace it, please refer to the document below.

“GENESIS64 - How to replace MC Works64 with GENESIS64” (Japanese Only)
(https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf)

<Customers using GENESIS>

Please download and install the latest product described in “Countermeasures for Products.”

Countermeasures for Products

CVE-2025-14815

<GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX>

The fixed version is as follows.

・ ICONICS Suite Version 10.98 or later*
Please download from the link below.
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

*GENESIS64, MobileHMI, Hyper Historian, and AnalytiX are included in the ICONICS Suite installation.

<MC Works64>

There are no plans to release a fixed version.

<GENESIS>

The fixed version is as follows.

・ GENESIS Version 11.03 or later
Please download from the link below.

[3] https://cwe.mitre.org/data/definitions/317.html

https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

CVE-2025-14816
<GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX>
The fixed version is as follows.
・ ICONICS Suite Version 10.98 or later*
Please download from the link below.
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

*GENESIS64, MobileHMI, Hyper Historian, and AnalytiX are included in the ICONICS Suite installation.

<MC Works64>
There are no plans to release a fixed version.

< GENESIS>
The fixed version is as follows.
・ GENESIS Version 11.03 or later
Please download from the link below.
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

Mitigations / Workarounds

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

All vulnerabilities
1) Use Windows authentication instead of SQL authentication for the SQL server authentication method.
2) Configure the PCs with the affected product installed so that only an administrator can log in.
3) Use the PCs with the affected product installed in the LAN and block remote login from untrusted networks and hosts, and from non-administrator users.
4) Block unauthorized access by using a firewall, virtual private network (VPN), etc. and allow remote login only to administrator when internet access is required.
5) Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
6) Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

CVE-2025-14815
1) In Workbench, open the “Configure Application(s) Settings” dialog. In the “Available Applications” list, uncheck the “Local Cache” column for applications and delete the files created by the local cache functionality from the following locations.

<GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, and AnalytiX>
C:¥ProgramData¥ICONICS¥Cache¥*.sdf

<MC Works64>
C:¥ProgramData¥ICONICS¥Cache¥*.sdf

<GENESIS>
C:¥ProgramData¥ICONICS¥11¥Cache¥*.sqlite3

CVE-2025-14816
1) Change the permissions of HHSplitter.exe so that only trusted administrators can execute it.
2) Delete HHSplitter.exe from the system if it is unnecessary.

Contact information

Please contact your local Mitsubishi Electric representative.

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