Overview
Information disclosure vulnerability due to reflected cross-site scripting (CWE-79) caused by the lack of proper input verification exists in MC Works64 mobile monitoring. An attacker may obtain authentication information of an MC Works64 server by injecting a malicious script in the URL of a monitoring screen delivered from the MC Works64 server to an application for mobile devices (MC Mobile) and leading a legitimate user to access this URL. And the attacker may perform any operation using the acquired authentication information. (CVE-2022-23127)

Versions of MC Works64 that are affected by this vulnerability are listed below, so please apply a security patch.

CVSS

Affected products
MC Works64 : Version 4.04E and prior

How to check the version
Open Windows® Control Panel and select “Programs and Features”. 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. 1).

<table>
<thead>
<tr>
<th>Name</th>
<th>Publisher</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELSOFT Help</td>
<td>MITSUBISHI ELECTRIC CORPORATION</td>
<td>10.95.210.00</td>
</tr>
<tr>
<td>MELSOFT MC Works64</td>
<td>MITSUBISHI ELECTRIC CORPORATION</td>
<td>10.95.210.01</td>
</tr>
<tr>
<td>MELSOFT MCDemo</td>
<td>MITSUBISHI ELECTRIC CORPORATION</td>
<td>10.95.210.00</td>
</tr>
</tbody>
</table>

Fig.1 MC Works64

Description
Information disclosure vulnerability due to reflected cross-site scripting (CWE-79) caused by the lack of proper input verification exists in MC Works64 mobile monitoring.

Impact
An attacker may obtain authentication information of an MC Works64 server by injecting a malicious script in the URL of a monitoring screen delivered from the MC Works64 server to an application for mobile devices (MC Mobile) and leading a legitimate user to access this URL. And the attacker may perform any operation using the acquired authentication information. (CVE-2022-23127)

Countermeasures
Please update your software by using the MC Works64 security patches. The following are instructions for downloading the security patches.


1) For Users using MC Works64 Version 4.04E

2) For Users using MC Works64 Edge-computing Edition Version 4.04E

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 1).

*1 This applies if the version number is from “10.95.201.23” to “10.95.209.08” in the version of “MELSOFT MC Works64”, which you can confirm in “How to check the version” of “Affected products”.

4) For Users using MC Works64 Version 3.04E

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 4).

*2 This applies if the version number is from “10.92.173.77” to “10.94.177.23” in the version of “MELSOFT MC Works64”, which you can confirm in “How to check the version” of “Affected products”.

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

*3 This applies if the version number is “10.87.148.42” or prior 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) Avoid clicking on web links in emails etc. from untrusted sources. Also, avoid opening files attached to untrusted emails.

Contact information
Please contact your local Mitsubishi Electric representative.

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