Denial of Service (DoS) and Remote Code Execution Vulnerability in MELSEC-Q/L Series Ethernet Interface Module and MELSEC iQ-R Series MES Interface Module

Release date: June 2, 2022
Mitsubishi Electric Corporation

Overview
Denial of Service (DoS) and Remote Code Execution Vulnerability exists in Web function on MELSEC-Q Ethernet Interface Module and MELSEC-L Ethernet Interface Module, and REST Server function on MELSEC iQ-R MES Interface Module. A remote unauthenticated attacker may cause a denial of service (DoS) condition or execute malicious code on target products by sending specially crafted packets (CVE-2022-25163).

The model names and firmware versions affected by this vulnerability are listed below. Please take measures based on the following Countermeasures or Mitigations/Workarounds.

CVSS

Affected products
Affected products and versions are below.

<table>
<thead>
<tr>
<th>Series</th>
<th>Product Name</th>
<th>Function Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELSEC-Q</td>
<td>QJ71E71-100</td>
<td>Web function</td>
<td>First 5 digits of serial number “24061” or prior.</td>
</tr>
<tr>
<td>MELSEC-L</td>
<td>LJ71E71-100</td>
<td>Web function</td>
<td>First 5 digits of serial number “24061” or prior.</td>
</tr>
<tr>
<td>MELSEC iQ-R</td>
<td>RD81MES96N</td>
<td>REST Server function</td>
<td>Firmware version “08” or prior</td>
</tr>
</tbody>
</table>

Please refer to the following manuals for how to check the serial number and version.
QJ71E71-100:
Q Corresponding Ethernet Interface Module User’s Manual (Basic) “Appendix 11 Checking the Serial Number and Function Version”
LJ71E71-100:
MELSEC-L Ethernet Interface Module User’s Manual (Basic) “Appendix 10 Checking the Serial Number, Function Version, and MAC address”
RD81MES96N:
MELSEC iQ-R Module Configuration Manual “Appendix 1 Checking Production Information and Firmware Version”

Description
Denial of Service (DoS) and Remote Code Execution Vulnerability due to Improper Input Validation (CWE-20) exists in Web function on MELSEC-Q Ethernet Interface Module and MELSEC-L Ethernet Interface Module, and REST Server function on MELSEC iQ-R MES Interface Module.

Impact
A remote unauthenticated attacker may cause a DoS condition or execute malicious code on target products by sending specially crafted packets. A system reset is required for recovery from a denial of service (DoS) condition and remote code execution.

Countermeasures
We have fixed the vulnerability at the following version.

<table>
<thead>
<tr>
<th>Series</th>
<th>Product Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELSEC-Q</td>
<td>QJ71E71-100</td>
<td>First 5 digits of serial number “24062” or later.</td>
</tr>
<tr>
<td>MELSEC-L</td>
<td>LJ71E71-100</td>
<td>First 5 digits of serial number “24062” or later.</td>
</tr>
<tr>
<td>MELSEC iQ-R</td>
<td>RD81MES96N</td>
<td>Firmware version “09” or later</td>
</tr>
</tbody>
</table>

Mitigations/Workarounds
Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:
- Use a firewall, virtual private network (VPN), web application firewall (WAF), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.

Contact information
Please contact your local Mitsubishi Electric representative.

Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html