Denial-of-Service Vulnerability in Robot Controller of MELFA FR Series and CR Series as well as ASSISTA

Release date: January 21, 2021
Last update date: May 18, 2021
Mitsubishi Electric Corporation

■ Overview
Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in a robot controller of MELFA FR Series and CR Series as well as cooperative robot ASSISTA due to a resource management errors (CWE-399). These robot controllers allow an attacker to cause a DoS of the execution of the robot program and the Ethernet communication by sending a large amount of packets in burst over a short period of time. As a result of DoS, an error may occur. (CVE-2021-20586)

The product models and firmware versions affected by this vulnerability are listed below.

■ CVSS
CVE-2021-20586 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■ Affected products
For the MELFA FR Series and CR Series as well as ASSISTA robot controllers, the model names and firmware versions in Table 1 are affected. Please refer to the next section for how to check the firmware version.

<table>
<thead>
<tr>
<th>Series</th>
<th>Model name</th>
<th>Controller model name</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELFA FR Series</td>
<td>RV-#FR$%W-D-@</td>
<td>CR800-#V$D</td>
<td>All Versions</td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-D-@</td>
<td>CR800-#HD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-D-@</td>
<td>CR800-#HRD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RV-#FR$%W-R-@</td>
<td>R16RTCPU +</td>
<td>CR800-#V$R</td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-R-@</td>
<td>R16RTCPU +</td>
<td>CR800-#HR</td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-R-@</td>
<td>R16RTCPU +</td>
<td>CR800-#HRR</td>
</tr>
<tr>
<td></td>
<td>RV-#FR$%W-Q-@</td>
<td>Q172DSRCPU +</td>
<td>CR800-#V$Q</td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-Q-@</td>
<td>Q172DSRCPU +</td>
<td>CR800-#HQ</td>
</tr>
<tr>
<td></td>
<td>RH-#FR$%W-Q-@</td>
<td>Q172DSRCPU +</td>
<td>CR800-#HRQ</td>
</tr>
<tr>
<td>MELFA CR Series</td>
<td>RV-8CRL-D-@</td>
<td>CR800-CVD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RH-#CRH$&amp;-D-@</td>
<td>CR800-CHD</td>
<td></td>
</tr>
<tr>
<td>MELFA ASSISTA</td>
<td>RV-5AS-D-@</td>
<td>CR800-05VD</td>
<td></td>
</tr>
</tbody>
</table>

#: Load capacity (Model name:2, 3, 4, 6, 7, 12, 13, 20 Controller model name:02, 03, 04, 06, 07, 12, 13, 20) 
$: Arm length (Model name RV type:L, LL or blank Model name RH type:35, 40, 45, 55, 60, 70, 85, 100 Controller model name:L or blank) 
%: Brake specification (B or blank) 
&: Vertical stroke (12, 15, 18, 20, 34, 35, 45) 
$: Environment specification (M, C, W or blank) 
@: Special device No. (S** or blank)

■ How to check the firmware version
- When using RT ToolBox3
When you select the [Online] section of the target project on the workspace screen (Figure 1(a)), you can check the firmware version on the property screen (Figure 1(b)).
- When using R32TB
  The firmware version can be checked on the title screen (Figure 2).

- When using R56TB
  The firmware version can be checked on the Version screen (Figure 3).

![Figure 2. How to check the firmware version with R32TB](image)

![Figure 3. How to check the firmware version with R56TB](image)

---

**Description**

A Denial of Service (DoS) vulnerability due to a resource management error (CWE-399) exists in the robot controllers of industrial robots MELFA FR series and CR series as well as ASSISTA.

**Impact**

Affected robot controllers allow an attacker to cause a DoS of the execution of the robot program and the Ethernet communication by sending a large amount of packets in burst over a short period of time. As a result of DoS, an error may occur. If the error occurs, the robot controller needs to be turned on again to recover.

**Countermeasures**

Please carry out the mitigations below.
Mitigations
Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use an IP filter function*1 and block access from untrusted networks and hosts.

*1 The product models and firmware versions support the IP filter function are listed below.

The product models and firmware versions:
- MELFA FR Series: firmware version “C2” or later
- MELFA CR Series: firmware version “C2” or later
- MELFA ASSISTA: firmware version “C2” or later

How to get the product supporting the IP filter function:
Please contact your local Mitsubishi Electric representative.

Acknowledgement
Mitsubishi Electric would like to thank Industrial Control Security Laboratory of Qi An Xin Group Inc. from China who reported this vulnerability.

Contact information
Please contact your local Mitsubishi Electric representative.

Update history
May 18, 2021
Modified the description of “Countermeasures”.
Added the IP filter function to “Mitigations”.