# Impact of Impersonation Vulnerability in TCP Protocol Stack

Release date: August 31, 2020
Last update date: June 13, 2024
Mitsubishi Electric Corporation

## Overview

There is a vulnerability in the TCP protocol stack of multiple our products that an attacker can impersonate the legitimate communication peer due to improper session management. If this vulnerability is exploited by an attacker, the attacker can impersonate a legitimate device and execute arbitrary commands, which may cause information disclosure, information tampering or destruction, and so on. (CVE-2020-16226)

The following are the names of products affected by this vulnerability, please take countermeasures or mitigations/workarounds. And the names of products affected by this vulnerability as well as countermeasures and mitigations/workarounds will be updated one by one.

## Description

Since the TCP protocol stack of multiple our products does not handle session management properly, an attacker can impersonate a legitimate device and execute arbitrary commands, which may cause information disclosure, information tampering or destruction, and so on. (CWE-342)

## Impact

If this vulnerability is exploited by an attacker, the attacker can impersonate a legitimate device and execute arbitrary commands, which may cause information disclosure, information tampering or destruction, and so on.

## Affected products, countermeasures, and mitigations or workarounds

[1] [Programmable Controllers-MELSEC]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| NZ2FT-MT, all versions<br>NZ2FT-EIP, all versions | <Countermeasures for Customers><br>There are no plans to release fixed versions. Customers using the affected products may take measures through mitigations and workarounds.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| Q03UDECPU, the first 5 digits of serial number 22081 and prior<br>Q24DHCCPU-V, the first 5 digits of serial number 24031 and prior<br>Q24DHCCPU-VG, the first 5 digits of serial number 24031 and prior<br>QnUDEHCPU(n=04/06/10/13/20/26/50/100), the first 5 digits of serial number 22081 and prior<br>QnUDVCPU(n=03/04/06/13/26), the first 5 digits of serial number 22031 and prior<br>QnUDPVCPU(n=04/06/13/26), the first 5 digits of serial number 22031 and prior<br>LnCPU(-P)(n=02/06/26), the first 5 digits of serial number 22051 and prior<br>L26CPU-(P)BT, the first 5 digits of serial number 22051 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available. Please consider migrating to MELSEC iQ-R Series.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- Q03UDECPU: The first 5 digits of serial number 22082 or later<br>- Q24DHCCPU-V: the first 5 digits of serial number 24032 or later<br>- Q24DHCCPU-VG: the first 5 digits of serial number 24032 or later<br>- QnUDEHCPU(n=04/06/10/13/20/26/50/100): the first 5 digits of serial number 22082 or later<br>- QnUDVCPU(n=03/04/06/13/26): the first 5 digits of serial number 22032 or later<br>- QnUDPVCPU(n=04/06/13/26): the first 5 digits of serial number 22032 or later<br>- LnCPU(-P)(n=02/06/26): he first 5 digits of serial number 22052 or later<br>- L26CPU-(P)BT: the first 5 digits of serial number 22052 or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| RnCPU(n=00/01/02), versions 18 and prior | <Countermeasures><br>Please update to version 19 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| RnCPU(n=04/08/16/32/120), versions 50 and prior<br>RnENCPU(n=04/08/16/32/120), versions 50 and prior | <Countermeasures><br>Please update to version 51 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| RnSFCPU (n=08/16/32/120), versions 22 and prior<br>RnPSFCPU(n=08/16/32/120), versions 05 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- RnSFCPU (n=08/16/32/120): version 23 or later<br>- RnPSFCPU(n=08/16/32/120): version 06 or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| RnPCPU(n=08/16/32/120), versions 24 and prior | <Countermeasures><br>Please update to version 25 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| R12CCPU-V, versions 13 and prior<br>RD55UP06-V, versions 09 and prior<br>RD55UP12-V, version 01 | <Countermeasures for Customers><br>If you are using the following versions, download the fixed version of firmware update file from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br>- R12CCPU-V, versions 09 to 13<br>- RD55UP06-V, versions 07 to 09<br>- RD55UP12-V, version 01<br><br>If you are using affected module R12CCPU-V (versions 08 and prior) or RD55UP06-V (versions 06 and prior), take measures through mitigations and workarounds. We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- R12CCPU-V: version 14 or later<br>- RD55UP06-V: version 10 or later<br>- RD55UP12-V: version 02 or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| Q06CCPU-V, all versions | <Countermeasures for Customers><br>Please consider migrating to Q12DCCPU-V or R12CCPU-V those are the successor models, because there are no plans to release the fixed version.<br><br>Or please carry out the mitigations below.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| RJ71GN11-T2, versions 11 and prior | <Countermeasures><br>Please update to version 12 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| RJ71EN71, version 48 and prior | <Countermeasures><br>Please update to version 49 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| RD78Gn(n=4,8,16,32,64), version 14 and prior<br>RD78GHV, version 14 and prior<br>RD78GHW, version 14 and prior | <Countermeasures><br>Please update to version 16 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| QJ71E71-100, the first 5 digits of serial number 21092 and prior<br>LJ71E71-100, the first 5 digits of serial number 21092 and prior<br>QJ71MT91, the first 5 digits of serial number 20082 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- QJ71E71-100: The first 5 digits of serial number 22102 or later<br>- LJ71E71-100: the first 5 digits of serial number 22102 or later<br>- QJ71MT91: the first 5 digits of serial number 22102 or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| QJ71MES96, all versions<br>QJ71WS96, all versions | <Countermeasures for Customers><br>Please carry out the mitigations below, because there are no plans to release the fixed versions or successor models.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| FX5U(C)-**M*/**<br>Case1: Serial number 17X**** or later: versions 1.210 and prior<br>Case2: Serial number 179**** and prior: versions 1.070 and prior | <Countermeasures><br>Case1: Please update to version 1.211 or later.<br>Case2: Please update to version 1.071 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| FX5UC-32M*/**-TS, versions 1.210 and prior | <Countermeasures><br>Please update to version 1.211 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| FX5UJ-**M*/**, version 1.000 | <Countermeasures><br>Please update to version 1.001 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| FX5-ENET, versions 1.002 and prior<br>FX5-ENET/IP, versions 1.002 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- FX5-ENET, version 1.003 or later<br>- FX5-ENET/IP, version 1.003 or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| FX5-CCLGN-MS, version 1.000 | <Countermeasures><br>Please update to version 1.001 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| FX3U-ENET-ADP, versions 1.22 and prior<br>FX3U-ENET, versions 1.14 and prior<br>FX3U-ENET-L, versions 1.14 and prior<br>FX3U-ENET-P502, versions 1.14 and prior<br>FX3GE-**M*/**, the first 3 digits of serial number 20X and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available. Please consider migrating to CPU modules of MELSEC iQ-F Series.<br><br><Countermeasures for Products><br>We have fixed the vulnerabilities at the following versions.<br>- FX3U-ENET-ADP, version 1.24 or later<br>- FX3U-ENET, version 1.16 or later<br>- FX3U-ENET-L, t version 1.16 or later<br>- FX3U-ENET-P502, version 1.16 or later<br>- FX3GE-**M*/**, the first 3 digits of serial number 20Y or later<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| NZ2GACP620-60, version 1.03D and prior<br>NZ2GACP620-300, version 1.03D and prior | <Countermeasures><br>Please update to version 1.04E or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊ Contact information

Please contact your local Mitsubishi Electric representative.

[2] [Data Logging Analyzer-MELQIC]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| IU1-1M20-D, all versions | <Countermeasures for Customers><br>Please carry out the mitigations below, because there are no plans to release the fixed version or successor models.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊ Contact information

Please contact your local Mitsubishi Electric representative.

[3] [Tension Controller]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| LE7-40GU-L,<br>screen package data, version 1.01 and prior | <Countermeasures><br>Please update to version 1.02 or later.<br>Contact your local Mitsubishi Electric representative for the fixed version of the screen package data and update it.<br><br><Mitigations/Workarounds><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊ Contact information

Please contact your local Mitsubishi Electric representative.

[4] [Human-Machine Interfaces-GOT]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| GOT1000 Series GT14 Model, all versions | <Countermeasures for Customers><br>Please migrate to GT2505(HS)-VTBD that is the successor model, because there are no plans to release the fixed version.<br><br>Or please carry out the mitigations below.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| GOT2000 Series GT21 Model, version 01.44.000 and prior<br>GS Series GS21 Model, version 01.44.000 and prior | <Countermeasures><br>Please update to version 01.45.000 or later.<br>Fixed firmware is included in GT Designer3 Version1(GOT2000) Ver.1.275M or later<br>Download the above version of GT Designer3 Version1(GOT2000) from the following site and update the firmware.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |
| GT25-J71GN13-T2, version 03 and prior | <Countermeasures><br>Please update to version 04 or later.<br>Download the fixed version of firmware from the following site and update it.<br>https://www.mitsubishielectric.com/fa/#software<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

* Contact information

Please contact your local Mitsubishi Electric representative.

[5] [Inverters-FREQROL]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| FR-A800-E Series, production date December, 2020 and prior<br>FR-F800-E Series, production date December, 2020 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>Products manufactured after January 2021 have been fixed.<br><br><Product Identification Method><br>Please check the serial number printed on the rating plate of inverter body or on the packaging plate of the inverter shipping carton.<br>[How to read the SERIAL number]<br>The second character of the serial indicates production year and the third character indicates production month.<br>The production year is the last digit of the year of manufacture, and the production month is indicated by 1 to 9, X (October), Y (November), or Z (December).<br>[The SERIAL number examples of fixed product]<br>*11******:for the product manufactured in January 2021<br>*12******:for the product manufactured in February 2021<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| FR-A8NCG, Production date August, 2020 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed version as shown below, but updating the product to the fixed version is not available.<br><br><Countermeasures for Products><br>Products manufactured after September 2020 have been fixed.<br><br><Product Identification Method><br>Please check the serial number printed on the rating plate of inverter body or on the packaging plate of the inverter shipping carton.<br><br>[How to read the SERIAL number]<br>The second character of the serial indicates production year and the third character indicates production month.<br>The production year is the last digit of the year of manufacture, and the production month is indicated by 1 to 9, X (October), Y (November), or Z (December).<br>[The SERIAL number examples of fixed product]<br>*09***:for the product manufactured in September 2020<br>*0X***:for the product manufactured in October 2020<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| FR-E800-EPA Series, Production date July, 2020 and prior<br>FR-E800-EPB Series, Production date July, 2020 and prior | <Countermeasures for Customers><br>Please take measures through mitigations and workarounds.<br>We have released the fixed versions as shown below, but updating the products to the fixed versions are not available.<br><br><Countermeasures for Products><br>Products manufactured after August 2020 have been fixed.<br><br><Product Identification Method><br>Please check the serial number printed on the rating plate of inverter body or on the packaging plate of the inverter shipping carton.<br><br>[How to read the SERIAL number]<br>The third and fourth characters of the serial indicate production year and the fifth character indicates production month.<br>The production year is the last two digits of the year of manufacture, and the production month is indicated by 1 to 9, X (October), Y (November), or Z (December).<br>[The SERIAL number examples of fixed product]<br>**208******:for the product manufactured in August 2020<br>**209******:for the product manufactured in September 2020<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊Contact information

Please contact your local Mitsubishi Electric representative.

[6] [Robots-MELFA]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| Conveyor Tracking Application<br>APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2), all versions<br>(Discontinued product) | <Countermeasures for Customers><br>Please carry out the mitigations below, because there are no plans to release the fixed versions or successor models.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊Contact information

Please contact your local Mitsubishi Electric representative.

[7] [AC Servos-MELSERVO]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| MR-J4-TM, all versions<br>MR-JE-C, all versions | <Countermeasures for Customers><br>Please carry out the mitigations below, because there are no plans to release the fixed versions or successor models.<br><br><Mitigations/Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.<br>- Use within a LAN and ensure that they are not accessible from untrusted networks and hosts.<br>- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet ports)<br>- Install an antivirus software in your personal computer that can access the product. |

＊Contact information

Please contact your local Mitsubishi Electric representative.

[8] [Air Conditioning]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| MSZ-BT20/25/35/50VGK-E1<br>MSZ-BT20/25/35/50VGK-ET1<br>MSZ-AP25/35/42/50/60/71VGK-E2<br>MSZ-AP25/35/42/50VGK-E7<br>MSZ-AP25/35/42/50VGK-EN2<br>MSZ-AP60/71VGK-ET2<br>MSZ-EF18/22/25/35/42/50VGKW(S)(B)-E1<br>MSZ-EF22/25/35/42/50VGKW(S)(B)-ER1<br>MSZ-EF25VGKB-ET1<br>MSZ-FT25/35/50VGK-E1<br>MSZ-FT25/35/50VGK-ET1<br>MSZ-FT25/35/50VGK-SC1<br>MSZ-EF22/25/35/42/50VGKW(S)(B)-A1<br>The above models of version 3000 or 3100.<br>"Version" is printed on Wi-Fi interface. | <Countermeasures><br>Recommended mitigation or workaround below.<br><br><Mitigations/Workarounds><br>1.Check if the router settings are as follows.<br>1-1. Set encryption key of wireless LAN which can hardly be identified. If key is changed from initial setting, avoid consecutive numbers and guessable MAC address, and combine letters and numbers.<br>1-2. Do not use WEP encryption algorithm or Open authentication.<br>1-3. If you change the router settings, hide its presence on the internet in order to make it difficult for unauthorized access.<br>(e.g. Set to not respond to PING request)<br>1-4. Set password for the router's Management portal, which is difficult to be identified.<br><br>2.Check the following when using a computer or tablet, etc. at home.<br>2-1. Update Antivirus software to the latest version.<br>2-2. Do not open or access suspicious attachment file or linked URL. |

＊Contact information

Please contact your local Mitsubishi Electric representative.

[9] [Air conditioning System / Centralized Controllers]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| G-50A, all versions<br>GB-50A, all versions<br>GB-24A, all versions<br>AG-150A, all versions<br>AG-150A-A, all versions<br>AG-150A-J, all versions<br>GB-50ADA-A, all versions<br>GB-50ADA-J, all versions | <Countermeasures><br>Please carry out the mitigations below.<br><br><Mitigations /Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet.<br>- Install an antivirus software in your personal computer that can access the product.<br>- Limit access to the products to trusted hosts only. |

＊Contact information:

Please contact your local Mitsubishi Electric representative.

[10] [Air conditioning System / Expansion Controllers]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| PAC-YG50ECA, all versions | <Countermeasures><br>Please carry out the mitigations below.<br><br><Mitigations /Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet.<br>- Install an antivirus software in your personal computer that can access the product.<br>- Limit access to the products to trusted hosts only. |

* Contact information:

Please contact your local Mitsubishi Electric representative.

[11] [Air conditioning System / BM adapter]

| Model | Countermeasures and Mitigations/Workarounds |
|---|---|
| BAC-HD150, versions 2.20 and prior | <Countermeasures><br>We have fixed the vulnerabilities at version 2.21 or later.<br>For versions 2.20 and prior, please carry out the mitigations below.<br><br><Mitigations /Workarounds><br>Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:<br>- Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet.<br>- Install an antivirus software in your personal computer that can access the product.<br>- Limit access to the products to trusted hosts only. |

* Contact information:

Please contact your local Mitsubishi Electric representative.

Acknowledgements

Mitsubishi Electric would like to thank Ta-Lun Yen of TXOne IoT/ICS Security Research Labs of Trend Micro working with Trend Micro’s Zero Day Initiative who reported this vulnerability.

Update history

June 13, 2024

Updated <Mitigations /Workarounds> for the following products

[1] All products
[2] All products
[3] All products
[4] All products
[5] All products
[6] All products
[7] All products

Revised <Countermeasures> for the following products to <Countermeasures for Customers> or <Countermeasures for Products>

[1] NZ2FT-MT, NZ2FT-EIP, Q03UDECPU, Q24DHCCPU-V, Q24DHCCPU-VG, QnUDEHCPU(n=04/06/10/13/20/26/50/100), QnUDVCPU(n=03/04/06/13/26), QnUDPVCPU(n=04/06/13/26), LnCPU(-P)(n=02/06/26), L26CPU-(P)BT, RnSFCPU(n=08/16/32/120), RnPSFCPU(n=08/16/32/120), R12CCPU-V, RD55UP06-V, RD55UP12-V, Q06CCPU-V, QJ71E71-100, LJ71E71-100, QJ71MT91, QJ71MES96, QJ71WS96, FX5-ENET, FX5-ENET/IP, FX5-CCLGN-MS, FX3UENET-ADP, FX3U-ENET, FX3U-ENET-L, FX3U-ENET-P502, FX3GE-**M*/**
[2] IU1-1M20-D
[4] GOT1000 Series GT14 Model
[5] FR-A800-E Series, FR-F800-E Series, FR-A8NCG, FR-E800-EPA Series, FR-E800-EPB Series
[6] Conveyor Tracking Application APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1/2)
[7] MR-J4-TM, MR-JE-C

June 29, 2023

Added countermeasures for the following products

[1] Q06CCPU-V, QJ71MES96, QJ71WS96

[2] IU1-1M20-D
[4] GOT1000 Series GT14 Model
[6] Conveyor Tracking Application: APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2)
[7] MR-J4-TM, MR-JE-C

September 22, 2022
Added fixed product as below
[3] LE7-40GU-L

May 24, 2022
Added fixed products as below
[1] Q24DHCCPU-V, Q24DHCCPU-VG
[4] GOT2000 Series GT21 Model, GS Series GS21 Model

August 24, 2021
Added fixed products as below
[1] RD78Gn(n=4,8,16,32,64), RD78GHV, RD78GHW

May 18, 2021
Added fixed products as below
[1] RJ71EN71, QJ71E71-100, LJ71E71-100, QJ71MT91, NZ2GACP620-60, NZ2GACP620-300
[4] GT25-J71GN13-T2

February 18, 2021
Add version information and/or fixed products as below
[8] MSZ-BT20/25/35/50VGK-E1, MSZ-BT20/25/35/50VGK-ET1, MSZ-AP25/35/42/50/60/71VGK-E2, MSZ-AP25/35/42/50VGK-E7, MSZ-AP25/35/42/50VGK-EN2, MSZ-AP60/71VGK-ET2, MSZ-EF18/22/25/35/42/50VGKW(S)(B)-E1, MSZ-EF22/25/35/42/50VGKW(S)(B)-ER1, MSZ-EF25VGKB-ET1, MSZ-FT25/35/50VGK-E1, MSZ-FT25/35/50VGK-ET1, MSZ-FT25/35/50VGK-SC1, MSZ-EF22/25/35/42/50VGKW(S)(B)-A1
[11] BAC-HD150

January 26, 2021
Added fixed products as below
[1] R12CCPU-V, RD55UP06-V, RD55UP12-V, RJ71GN11-T2, Q03UDECPU, QnUDEHCPU, QnUDVCPU, QnUDPVCPU
LnCPU(-P), L26CPU-(P)BT, RnSFCPU, RnPCPU, RnPSFCPU, FX5-ENET, FX5-ENET/IP, FX3U-ENET-ADP
FX3GE-**M*/**, FX3U-ENET, FX3U-ENET-L, FX3U-ENET-P502 and FX5-CCLGN-MS
[5]FR-A800-E Series, FR-F800-E Series, FR-A8NCG, FR-E800-EPA Series and FR-E800-EPB Series

September 24, 2020
Add affected products ([8] - [11])