Impact of Impersonation Vulnerability in TCP Protocol Stack

Release date: August 31, 2020
Last update date: September 24, 2020
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
QJ71MES96, all versions QJ71WS96, all versions Q06CCPU-V, all versions Q24DHCCPU-V, all versions Q24DHCCPU-VG, all versions R12CCPU-V, all versions RD55UP06-V, all versions RD55UP12-V, all versions RJ71GN11-T2, all versions RJ71EN71, all versions QJ71E71-100, all versions LJ71E71-100, all versions QJ71MT91, all versions RD78Gn(n=4,8,16,32,64), all versions RD78GHV, all versions RD78GHW, all versions NZ2GACP620-60, all versions NZ2GACP620-300, all versions NZ2FT-MT, all versions NZ2FT-EIP, all versions Q03UDECPU, the first 5 digits of serial number 22081 and prior QnUDEHCPU(n=04/06/10/13/20/26/50/100), the first 5 digits of serial number 22081 and prior QnUDVCPU(n=03/04/06/13/26), the first 5 digits of serial number 22031 and prior QnUDPVCPU(n=04/06/13/2), the first 5 digits of serial number 22031 and prior LnCPU(-P)(n=02/06/26), the first 5 digits of serial number 22051 and prior L26CPU-(P)BT, the first 5 digits of serial number 22051 and prior	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - Install an antivirus software in your personal computer that can access the product.

Model	Countermeasures and Mitigations/Workarounds
RnCPU(n=00/01/02), versions 18 and prior	<Countermeasures> Please update to version 19 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. – Install an antivirus software in your personal computer that can access the product.
RnCPU(n=04/08/16/32/120), versions 50 and prior	<Countermeasures> Please update to version 51 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. – Install an antivirus software in your personal computer that can access the product.
RnENCPU(n=04/08/16/32/120), versions 50 and prior	<Countermeasures> Please update to version 51 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. – Install an antivirus software in your personal computer that can access the product.
RnSFCPU (n=08/16/32/120), all versions RnPCPU(n=08/16/32/120), all versions RnPSFCPU(n=08/16/32/120), all versions	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. – Install an antivirus software in your personal computer that can access the product.

Model	Countermeasures and Mitigations/Workarounds
FX5U(C)-**M*/** Case1: Serial number 17X**** or later: versions 1.210 and prior Case2 Serial number 179**** and prior: versions 1.070 and prior	<Countermeasures> Case1: Please update to version 1.211 or later. Case2 Please update to version 1.071 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - Install an antivirus software in your personal computer that can access the product.
FX5UC-32M*/**-TS, Ver. 1.210 and prior	<Countermeasures> Please update to version 1.211 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - Install an antivirus software in your personal computer that can access the product.
FX5UJ-**M*/**, version 1.000	<Countermeasures> Please update to version 1.001 or later. Download the fixed version of software product from the following site and update it. https://www.mitsubishielectric.com/fa/#software <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - Install an antivirus software in your personal computer that can access the product.
FX5-ENET, all versions FX5-ENET/IP, all versions FX3U-ENET-ADP, all versions FX3GE-**M*/**, all versions FX3U-ENET, all versions FX3U-ENET-L, all versions FX3U-ENET-P502, all versions FX5-CCLGN-MS, all versions	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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, all versions	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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
GOT2000 Series GT21 Model, all versions GS Series, all versions GOT1000 Series GT14 Model, all versions GT25-J71GN13-T2, all versions	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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, all versions FR-F800-E Series, all versions FR-A8NCG, Production date August, 2020 and prior FR-E800-EPA Series, Production date July, 2020 and prior FR-E800-EPB Series, Production date July, 2020 and prior	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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 APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2), all versions (Discontinued product)	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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 MR-JE-C, all versions	<Countermeasures> Please carry out the workaround below. <Mitigations/Workarounds> 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 ensure that they are not accessible from untrusted networks and hosts. - 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 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	<Countermeasures> Recommended mitigation or workaround below. <Mitigations/Workarounds> 1.Check if the router settings are as follows. 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. 1-2. Do not use WEP encryption algorithm or Open authentication. 1-3. If you change the router settings, hide its presence on the internet in order to make it difficult for unauthorized access. (e.g. Set to not respond to PING request) 1-4. Set password for the router's Management portal, which is difficult to be identified. 2.Check the following when using a computer or tablet, etc. at home. 2-1. Update Antivirus software to the latest version. 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 GB-50A All versions GB-24A All versions AG-150A All versions AG-150A-A All versions AG-150A-J All versions GB-50ADA-A All versions GB-50ADA-J All versions	<Countermeasures> Please carry out the workaround below. <Mitigations /Workarounds> Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability: - Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet. - Install an antivirus software in your personal computer that can access the product. - 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> Please carry out the workaround below. <Mitigations /Workarounds> Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability: - Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet. - Install an antivirus software in your personal computer that can access the product. - 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	<Countermeasures> Please carry out the workaround below. <Mitigations /Workarounds> Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability: - Use the products securely with VPN, routers or other ways when the products are connected to external network such as the Internet. - Install an antivirus software in your personal computer that can access the product. - 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
September 24, 2020
Add affected products ([8] - [11])