

Denial-of-Service(DoS) Vulnerability and Client-side Script Injection Vulnerability in multiple consumer electronics products

Release date: September 29, 2022
Mitsubishi Electric Corporation

■ Overview

A Denial of Service (DoS) vulnerability due to use of freed memory (CWE-416) and a client-side script injection vulnerability due to cross-site scripting (CWE-79) exist in multiple consumer electronics products manufactured by Mitsubishi Electric Corporation. These vulnerabilities allow a malicious attacker to cause a DoS Condition (CVE-2022-29859) on the products or make it respond with a message containing an arbitrary malicious script, which may be executed on the browser, resulting in information disclosure, etc. (CVE-2022-33322). The following products are affected by these vulnerabilities, please take countermeasures, mitigations and workarounds.

■ CVSS Score

CVE-2022-29859 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score:3.1

CVE-2022-33322 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N Base Score:6.8

■ Description

Multiple consumer electronics products manufactured by Mitsubishi Electric have a Denial of Service (DoS) vulnerability (CVE-2022-29859) due to the following defect in a DHCP process in OSS (open source software) and a client-side script injection vulnerability (CVE-2022-33322) due to the following defect caused by improper input filtering/validation on a web server.

CVE-2022-29859: Use of freed memory (CWE-416)

CVE-2022-33322: Cross-site scripting (CWE-79)

■ Impact

An attacker can cause a DoS Condition by sending specially crafted message to the target device, or making it respond with a message containing an arbitrary malicious script, which may be executed on the browser, resulting in information disclosure, etc.

■ Affected products, countermeasures, and mitigations or workarounds

[1] [Wi-Fi Interface and Air Conditioning]

model number	Countermeasures and Mitigation/Workarounds
<p><u>Wi-Fi Interface:</u> MAC-587IF-E MAC-587IF2-E MAC-507IF-E MAC-588IF-E S-MAC-002IF</p> <p><u>Air Conditioning:</u> MSXY-FP05/07/10/13/18/20/24VGK-SG1 MSY-GP10/13/15/18/20/24VFK-SG1 MSZ-AP25/35/42/50VGK-E1 MSZ-AP15/20/25/35/42/50/60/71VGK-E2 MSZ-AP25/35/42/50/60/71VGK-E3 MSZ-AP25/35/42/50VGK-E7 MSZ-AP25/35/42/50VGK-E8 MSZ-AP25/35/42/50VGK-EN1 MSZ-AP25/35/42/50VGK-EN2 MSZ-AP25/35/42/50VGK-EN3 MSZ-AP25/35/42/50VGK-ER1 MSZ-AP15/20/25/35/42/50/60/71VGK-ER2 MSZ-AP25/35/42/50/60/71VGK-ER3 MSZ-AP25/35/42/50VGK-ET1 MSZ-AP15/20/25/35/42/50/60/71VGK-ET2 MSZ-AP25/35/42/50/60/71VGK-ET3 MSZ-AY25/35/42/50VGK-E1 MSZ-AY25/35/42/50VGK-E6 MSZ-AY25/35/42/50VGK-ER1 MSZ-AY25/35/42/50VGK-ET1 MSZ-AY25/35/42/50VGK-SC1 MSZ-AY25/35/42/50VGKP-E6 MSZ-AY25/35/42/50VGKP-ER1 MSZ-AY25/35/42/50VGKP-ET1 MSZ-AY25/35/42/50VGKP-SC1 MSZ-BT20/25/35/50VGK-E1 MSZ-BT20/25/35/50VGK-E2 MSZ-BT20/25/35/50VGK-E3 MSZ-BT20/25/35/50VGK-ER1 MSZ-BT20/25/35/50VGK-ER2 MSZ-BT20/25/35/50VGK-ET1 MSZ-BT20/25/35/50VGK-ET2 MSZ-BT20/25/35/50VGK-ET3 MSZ-EF18/22/25/35/42/50VGKW-E1 MSZ-EF18/22/25/35/42/50VGKB-E1 MSZ-EF18/22/25/35/42/50VGKS-E1 MSZ-EF18/22/25/35/42/50VGKW-E2 MSZ-EF18/22/25/35/42/50VGKB-E2 MSZ-EF18/22/25/35/42/50VGKS-E2 MSZ-EF22/25/35/42/50VGKW-ER1 MSZ-EF22/25/35/42/50VGKB-ER1 MSZ-EF22/25/35/42/50VGKS-ER1 MSZ-EF22/25/35/42/50VGKW-ER2 MSZ-EF22/25/35/42/50VGKB-ER2 MSZ-EF22/25/35/42/50VGKS-ER2 MSZ-EF22/25/35/42/50VGKW-ET1 MSZ-EF22/25/35/42/50VGKB-ET1 MSZ-EF22/25/35/42/50VGKS-ET1 MSZ-EF22/25/35/42/50VGKW-ET2 MSZ-EF22/25/35/42/50VGKB-ET2 MSZ-EF22/25/35/42/50VGKS-ET2 MSZ-FT25/35/50VGK-E1 MSZ-FT25/35/50VGK-E2 MSZ-FT25/35/50VGK-ET1 MSZ-FT25/35/50VGK-SC1</p>	<p><Impact> These vulnerabilities allow a malicious attacker to cause a DoS Condition on the products or make it respond with a message containing an arbitrary malicious script, which may be executed on the browser, resulting in information disclosure, etc.</p> <p><Countermeasures> Please carry out the mitigations below.</p> <p><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. 1-5. Install the wireless LAN router in a location where it cannot be touched by outsiders. Do not open the network to unspecified third parties, such as by offering it as free Wi-Fi. 1-6. Do not let any third parties know the URL (IP address or host name) of the relevant product.</p> <p>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.</p>

MSZ-FT25/35/50VGK-SC2
MSZ-HR25/35/42/50/60/71VFK-E1
MSZ-HR25/35/42/50VFK-E6
MSZ-HR25/35/42/50/60/71VFK-ER1
MSZ-HR25/35/42/50/60/71VFK-ET1
MSZ-LN18/25/35/50/60VG2W-E2
MSZ-LN18/25/35/50/60VG2W-E3
MSZ-LN25/35/50VG2W-EN2
MSZ-LN18/25/35/50/60VG2W-ER2
MSZ-LN25/35/50/60VG2W-ER3
MSZ-LN18/25/35/50/60VG2W-ET2
MSZ-LN25/35/50/60VG2W-ET3
MSZ-LN18/25/35/50/60VG2V-E2
MSZ-LN18/25/35/50/60VG2V-E3
MSZ-LN25/35/50VG2V-EN2
MSZ-LN25/35/50/60VG2V-ER2
MSZ-LN25/35/50/60VG2V-ER3
MSZ-LN25/35/50/60VG2V-ET2
MSZ-LN25/35/50/60VG2V-ET3
MSZ-LN18/25/35/50/60VG2B-E2
MSZ-LN18/25/35/50/60VG2B-E3
MSZ-LN25/35/50VG2B-EN2
MSZ-LN25/35/50/60VG2B-ER2
MSZ-LN25/35/50/60VG2B-ER3
MSZ-LN25/35/50/60VG2B-ET2
MSZ-LN25/35/50/60VG2B-ET3
MSZ-LN18/25/35/50/60VG2R-E2
MSZ-LN18/25/35/50/60VG2R-E3
MSZ-LN25/35/50VG2R-EN2
MSZ-LN25/35/50/60VG2R-ER2
MSZ-LN25/35/50/60VG2R-ER3
MSZ-LN25/35/50/60VG2R-ET2
MSZ-LN25/35/50/60VG2R-ET3
MSZ-LN18/25/35/50VG2W-SC1
MSZ-LN25/35/50VG2V-SC1
MSZ-LN25/35/50VG2B-SC1
MSZ-LN25/35/50VG2R-SC1
MSZ-RW25/35/50VG-E1
MSZ-RW25/35/50VG-ER1
MSZ-RW25/35/50VG-ET1
MSZ-RW25/35/50VG-SC1
MSZ-AP22/25/35/42/50/61/70/80VGKD-A1
MSZ-AP22/25/35/42/50/60/71/80VGKD-A2
MSZ-EF22/25/35/42/50VGKW-A1
MSZ-EF22/25/35/42/50VGKB-A1
MSZ-EF22/25/35/42/50VGKS-A1
MSZ-LN25/35/50/60VG2V-A2
MSZ-LN25/35/50/60VG2B-A2
MSZ-LN25/35/50/60VG2R-A2
MFZ-GXT50/60/73VFK
MFZ-XT50/60VFK
MSZ-EZA09/12VAK
MSZ-EXA09/12VAK
MSZ-GZY09/12/18VFK
MSZ-KY09/12/18VFK
MSZ-WX18/20/25VFK
MSZ-ZY09/12/18VFK

Versions 35.00 and prior of the above models are affected.

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries> <https://www.mitsubishielectric.com/en/contact/room-air-conditioners.html>

[2] [Air Purifier]

model number	Countermeasures and Mitigation/Workarounds
<p>MA-EW85S-E MA-EW85S-UK</p> <p>Versions 80.00 and prior of the above models are affected.</p>	<p><Impact> These vulnerabilities allow a malicious attacker to cause a DoS Condition on the products or make it respond with a message containing an arbitrary malicious script, which may be executed on the browser, resulting in information disclosure, etc.</p> <p><Countermeasures> Please carry out the mitigations below.</p> <p><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. 1-5. Install the wireless LAN router in a location where it cannot be touched by outsiders. Do not open the network to unspecified third parties, such as by offering it as free Wi-Fi. 1-6. Do not let any third parties know the URL (IP address or host name) of the relevant product.</p> <p>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.</p>

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries> <https://www.mitsubishielectric.com/en/products-solutions/home/index.html>