

# Denial-of-Service (DoS) Vulnerability due to Realtek chips Vulnerability in Wi-Fi connection process in access point mode for multiple consumer electronics products

Release date: November 15, 2022  
Mitsubishi Electric Corporation

## ■ Overview

A Denial-of-Service (DoS) vulnerability caused by deadlock (CWE-833)<sup>1</sup> due to Realtek chips vulnerability (CVE-2022-34326) in the Wi-Fi connection process in access point mode exists in consumer electronics products by manufactured Mitsubishi Electric Corporation. The access point mode is for connecting our products to an external connection device (wireless LAN router) during device registration. If the product receives data specially crafted by a malicious attacker within range of Wi-Fi communication, Wi-Fi communication of the product operating in access point mode may temporarily result in a DoS condition and suspend. As a result, device registration may become impossible. The names of the products affected by this vulnerability are listed in "Affected products, countermeasures, and mitigations or workarounds" section, please take countermeasures, mitigations and workarounds.

This vulnerability does not cause information disclosure of personal information or equipment data, or unauthorized operation of equipment. In addition, the following products or user environments are not affected by this vulnerability.

- Products that do not support Wi-Fi communication
- When not using a Wi-Fi communication with a product that supports Wi-Fi communication
- Using a WPS communication with a product that supports Wi-Fi communication
- When using a Wi-Fi communication normally with a product that supports Wi-Fi communication after completing device registration

## ■ CVSS Score<sup>2</sup>

CVE-2022-34326 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score:3.1

## ■ Description

A Denial-of-Service (DoS) vulnerability due to deadlock (CWE-833) in the Wi-Fi connection process in access point mode exists in consumer electronics products by manufactured Mitsubishi Electric Corporation (CVE-2022-34326). The access point mode is the mode used for device registration. Under normal conditions of use, the access point mode is not used and the product is not affected by this vulnerability.

## ■ Impact

If the product receives data specially crafted by a malicious attacker within range of Wi-Fi communication, Wi-Fi communication of the product operating in access point mode may temporarily result in a DoS condition and suspend. As a result, device registration may become impossible. If the product results in a DoS condition, it can be recovered by manually restarting it. After recovery, you can register the device again.

<sup>1</sup> <https://cwe.mitre.org/data/definitions/833.html>

<sup>2</sup> <https://www.first.org/cvss/v3.1/specification-document>

■ 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-5871F-E            MAC-5871F2-E            MAC-5071F-E            MAC-5881F-E            S-MAC-0021F</p> <p><u>Air Conditioning:</u>            MSXY-FP05VGK-SG1            MSXY-FP07VGK-SG1            MSXY-FP10VGK-SG1            MSXY-FP13VGK-SG1            MSXY-FP18VGK-SG1            MSXY-FP20VGK-SG1            MSXY-FP24VGK-SG1            MSY-GP10VFK-SG1            MSY-GP13VFK-SG1            MSY-GP15VFK-SG1            MSY-GP18VFK-SG1            MSY-GP20VFK-SG1            MSY-GP24VFK-SG1            MSZ-AP15VGK-E1            MSZ-AP15VGK-E2            MSZ-AP15VGK-ER1            MSZ-AP15VGK-ER2            MSZ-AP15VGK-ET1            MSZ-AP15VGK-ET2            MSZ-AP20VGK-E1            MSZ-AP20VGK-E2            MSZ-AP20VGK-ER1            MSZ-AP20VGK-ER2            MSZ-AP20VGK-ET1            MSZ-AP20VGK-ET2            MSZ-AP25VGK-E1            MSZ-AP25VGK-E2            MSZ-AP25VGK-E3            MSZ-AP25VGK-E7            MSZ-AP25VGK-E8            MSZ-AP25VGK-EN1            MSZ-AP25VGK-EN2            MSZ-AP25VGK-EN3            MSZ-AP25VGK-ER1            MSZ-AP25VGK-ER2            MSZ-AP25VGK-ER3            MSZ-AP25VGK-ET1            MSZ-AP25VGK-ET2            MSZ-AP25VGK-ET3            MSZ-AP35VGK-E1            MSZ-AP35VGK-E2            MSZ-AP35VGK-E3            MSZ-AP35VGK-E7            MSZ-AP35VGK-E8            MSZ-AP35VGK-EN1            MSZ-AP35VGK-EN2            MSZ-AP35VGK-EN3            MSZ-AP35VGK-ER1            MSZ-AP35VGK-ER2            MSZ-AP35VGK-ER3            MSZ-AP35VGK-ET1            MSZ-AP35VGK-ET2            MSZ-AP35VGK-ET3            MSZ-AP42VGK-E1            MSZ-AP42VGK-E2</p>	<p>&lt;Impact&gt;            If the product receives data specially crafted by a malicious attacker within range of Wi-Fi communication, Wi-Fi communication of the product operating in access point mode may temporarily result in a DoS condition and suspend. As a result, device registration may become impossible.</p> <p>&lt;Countermeasures&gt;            Please carry out the mitigations below.</p> <p>&lt;Mitigations/Workarounds&gt;            Make sure that the SSID and KEY of the access point mode of the affected product are not known to an unspecified third party.</p> <p>When using a PC, tablet or other device at home, please check the following.</p> <ul style="list-style-type: none"> <li>- Please update your OS, software, anti-virus software, etc. to the latest version before use.</li> <li>- Do not open attachments or hyperlinks from unreliable sources or of unknown origin.</li> </ul>

MSZ-AP42VGK-E3	
MSZ-AP42VGK-E7	
MSZ-AP42VGK-E8	
MSZ-AP42VGK-EN1	
MSZ-AP42VGK-EN2	
MSZ-AP42VGK-EN3	
MSZ-AP42VGK-ER1	
MSZ-AP42VGK-ER2	
MSZ-AP42VGK-ER3	
MSZ-AP42VGK-ET1	
MSZ-AP42VGK-ET2	
MSZ-AP42VGK-ET3	
MSZ-AP50VGK-E1	
MSZ-AP50VGK-E2	
MSZ-AP50VGK-E3	
MSZ-AP50VGK-E7	
MSZ-AP50VGK-E8	
MSZ-AP50VGK-EN1	
MSZ-AP50VGK-EN2	
MSZ-AP50VGK-EN3	
MSZ-AP50VGK-ER1	
MSZ-AP50VGK-ER2	
MSZ-AP50VGK-ER3	
MSZ-AP50VGK-ET1	
MSZ-AP50VGK-ET2	
MSZ-AP50VGK-ET3	
MSZ-AP60VGK-E2	
MSZ-AP60VGK-E3	
MSZ-AP60VGK-E4	
MSZ-AP60VGK-ER2	
MSZ-AP60VGK-ER3	
MSZ-AP60VGK-ER4	
MSZ-AP60VGK-ET2	
MSZ-AP60VGK-ET3	
MSZ-AP60VGK-ET4	
MSZ-AP71VGK-E2	
MSZ-AP71VGK-E3	
MSZ-AP71VGK-E4	
MSZ-AP71VGK-ER2	
MSZ-AP71VGK-ER3	
MSZ-AP71VGK-ER4	
MSZ-AP71VGK-ET2	
MSZ-AP71VGK-ET3	
MSZ-AP71VGK-ET4	
MSZ-AY25VGK-E1	
MSZ-AY25VGK-E6	
MSZ-AY25VGK-ER1	
MSZ-AY25VGK-ET1	
MSZ-AY25VGKP-E1	
MSZ-AY25VGKP-E6	
MSZ-AY25VGKP-ER1	
MSZ-AY25VGKP-ET1	
MSZ-AY25VGKP-SC1	
MSZ-AY25VGK-SC1	
MSZ-AY35VGK-E1	
MSZ-AY35VGK-E6	
MSZ-AY35VGK-ER1	
MSZ-AY35VGK-ET1	
MSZ-AY35VGKP-E1	
MSZ-AY35VGKP-E6	
MSZ-AY35VGKP-ER1	
MSZ-AY35VGKP-ET1	
MSZ-AY35VGKP-SC1	
MSZ-AY35VGK-SC1	
MSZ-AY42VGK-E1	

MSZ-AY42VGK-E6	
MSZ-AY42VGK-ER1	
MSZ-AY42VGK-ET1	
MSZ-AY42VGKP-E1	
MSZ-AY42VGKP-E6	
MSZ-AY42VGKP-ER1	
MSZ-AY42VGKP-ET1	
MSZ-AY42VGKP-SC1	
MSZ-AY42VGK-SC1	
MSZ-AY50VGK-E1	
MSZ-AY50VGK-E6	
MSZ-AY50VGK-ER1	
MSZ-AY50VGK-ET1	
MSZ-AY50VGKP-E1	
MSZ-AY50VGKP-E6	
MSZ-AY50VGKP-ER1	
MSZ-AY50VGKP-ET1	
MSZ-AY50VGKP-SC1	
MSZ-AY50VGK-SC1	
MSZ-BT20VGK-E1	
MSZ-BT20VGK-E2	
MSZ-BT20VGK-E3	
MSZ-BT20VGK-ER1	
MSZ-BT20VGK-ER2	
MSZ-BT20VGK-ET1	
MSZ-BT20VGK-ET2	
MSZ-BT20VGK-ET3	
MSZ-BT25VGK-E1	
MSZ-BT25VGK-E2	
MSZ-BT25VGK-E3	
MSZ-BT25VGK-ER1	
MSZ-BT25VGK-ER2	
MSZ-BT25VGK-ET1	
MSZ-BT25VGK-ET2	
MSZ-BT25VGK-ET3	
MSZ-BT35VGK-E1	
MSZ-BT35VGK-E2	
MSZ-BT35VGK-E3	
MSZ-BT35VGK-ER1	
MSZ-BT35VGK-ER2	
MSZ-BT35VGK-ET1	
MSZ-BT35VGK-ET2	
MSZ-BT35VGK-ET3	
MSZ-BT50VGK-E1	
MSZ-BT50VGK-E2	
MSZ-BT50VGK-E3	
MSZ-BT50VGK-ER1	
MSZ-BT50VGK-ER2	
MSZ-BT50VGK-ET1	
MSZ-BT50VGK-ET2	
MSZ-BT50VGK-ET3	
MSZ-EF18VGKB-E1	
MSZ-EF18VGKB-E2	
MSZ-EF18VGKS-E1	
MSZ-EF18VGKS-E2	
MSZ-EF18VGKW-E1	
MSZ-EF18VGKW-E2	
MSZ-EF22VGKB-E1	
MSZ-EF22VGKB-E2	
MSZ-EF22VGKB-ER1	
MSZ-EF22VGKB-ER2	
MSZ-EF22VGKB-ET1	
MSZ-EF22VGKB-ET2	
MSZ-EF22VGKS-E1	
MSZ-EF22VGKS-E2	

MSZ-EF22VGKS-ER1	
MSZ-EF22VGKS-ER2	
MSZ-EF22VGKS-ET1	
MSZ-EF22VGKS-ET2	
MSZ-EF22VGKW-E1	
MSZ-EF22VGKW-E2	
MSZ-EF22VGKW-ER1	
MSZ-EF22VGKW-ER2	
MSZ-EF22VGKW-ET1	
MSZ-EF22VGKW-ET2	
MSZ-EF25VGKB-E1	
MSZ-EF25VGKB-E2	
MSZ-EF25VGKB-ER1	
MSZ-EF25VGKB-ER2	
MSZ-EF25VGKB-ET1	
MSZ-EF25VGKB-ET2	
MSZ-EF25VGKS-E1	
MSZ-EF25VGKS-E2	
MSZ-EF25VGKS-ER1	
MSZ-EF25VGKS-ER2	
MSZ-EF25VGKS-ET1	
MSZ-EF25VGKS-ET2	
MSZ-EF25VGKW-E1	
MSZ-EF25VGKW-E2	
MSZ-EF25VGKW-ER1	
MSZ-EF25VGKW-ER2	
MSZ-EF25VGKW-ET1	
MSZ-EF25VGKW-ET2	
MSZ-EF35VGKB-E1	
MSZ-EF35VGKB-E2	
MSZ-EF35VGKB-ER1	
MSZ-EF35VGKB-ER2	
MSZ-EF35VGKB-ET1	
MSZ-EF35VGKB-ET2	
MSZ-EF35VGKS-E1	
MSZ-EF35VGKS-E2	
MSZ-EF35VGKS-ER1	
MSZ-EF35VGKS-ER2	
MSZ-EF35VGKS-ET1	
MSZ-EF35VGKS-ET2	
MSZ-EF35VGKW-E1	
MSZ-EF35VGKW-E2	
MSZ-EF35VGKW-ER1	
MSZ-EF35VGKW-ER2	
MSZ-EF35VGKW-ET1	
MSZ-EF35VGKW-ET2	
MSZ-EF42VGKB-E1	
MSZ-EF42VGKB-E2	
MSZ-EF42VGKB-ER1	
MSZ-EF42VGKB-ER2	
MSZ-EF42VGKB-ET1	
MSZ-EF42VGKB-ET2	
MSZ-EF42VGKS-E1	
MSZ-EF42VGKS-E2	
MSZ-EF42VGKS-ER1	
MSZ-EF42VGKS-ER2	
MSZ-EF42VGKS-ET1	
MSZ-EF42VGKS-ET2	
MSZ-EF42VGKW-E1	
MSZ-EF42VGKW-E2	
MSZ-EF42VGKW-ER1	
MSZ-EF42VGKW-ER2	
MSZ-EF42VGKW-ET1	
MSZ-EF42VGKW-ET2	
MSZ-EF50VGKB-E1	

MSZ-EF50VGKB-E2	
MSZ-EF50VGKB-ER1	
MSZ-EF50VGKB-ER2	
MSZ-EF50VGKB-ET1	
MSZ-EF50VGKB-ET2	
MSZ-EF50VGKS-E1	
MSZ-EF50VGKS-E2	
MSZ-EF50VGKS-ER1	
MSZ-EF50VGKS-ER2	
MSZ-EF50VGKS-ET1	
MSZ-EF50VGKS-ET2	
MSZ-EF50VGKW-E1	
MSZ-EF50VGKW-E2	
MSZ-EF50VGKW-ER1	
MSZ-EF50VGKW-ER2	
MSZ-EF50VGKW-ET1	
MSZ-EF50VGKW-ET2	
MSZ-FT25VGK-E1	
MSZ-FT25VGK-E2	
MSZ-FT25VGK-ET1	
MSZ-FT25VGK-SC1	
MSZ-FT25VGK-SC2	
MSZ-FT35VGK-E1	
MSZ-FT35VGK-E2	
MSZ-FT35VGK-ET1	
MSZ-FT35VGK-SC1	
MSZ-FT35VGK-SC2	
MSZ-FT50VGK-E1	
MSZ-FT50VGK-E2	
MSZ-FT50VGK-ET1	
MSZ-FT50VGK-SC1	
MSZ-FT50VGK-SC2	
MSZ-HR25VFK-E1	
MSZ-HR25VFK-E6	
MSZ-HR25VFK-E7	
MSZ-HR25VFK-ER1	
MSZ-HR25VFK-ET1	
MSZ-HR35VFK-E1	
MSZ-HR35VFK-E6	
MSZ-HR35VFK-E7	
MSZ-HR35VFK-ER1	
MSZ-HR35VFK-ET1	
MSZ-HR42VFK-E1	
MSZ-HR42VFK-E6	
MSZ-HR42VFK-E7	
MSZ-HR42VFK-ER1	
MSZ-HR42VFK-ET1	
MSZ-HR50VFK-E1	
MSZ-HR50VFK-E6	
MSZ-HR50VFK-E7	
MSZ-HR50VFK-ER1	
MSZ-HR50VFK-ET1	
MSZ-HR60VFK-E1	
MSZ-HR60VFK-ER1	
MSZ-HR60VFK-ET1	
MSZ-HR71VFK-E1	
MSZ-HR71VFK-ER1	
MSZ-HR71VFK-ET1	
MSZ-LN18VG2B-E2	
MSZ-LN18VG2B-E3	
MSZ-LN18VG2R-E2	
MSZ-LN18VG2R-E3	
MSZ-LN18VG2V-E2	
MSZ-LN18VG2V-E3	
MSZ-LN18VG2W-E2	

MSZ-LN18VG2W-E3	
MSZ-LN18VG2W-ER2	
MSZ-LN18VG2W-ET2	
MSZ-LN18VG2W-SC1	
MSZ-LN25VG2B-E2	
MSZ-LN25VG2B-E3	
MSZ-LN25VG2B-EN2	
MSZ-LN25VG2B-ER2	
MSZ-LN25VG2B-ER3	
MSZ-LN25VG2B-ET2	
MSZ-LN25VG2B-ET3	
MSZ-LN25VG2B-SC1	
MSZ-LN25VG2R-E2	
MSZ-LN25VG2R-E3	
MSZ-LN25VG2R-EN2	
MSZ-LN25VG2R-ER2	
MSZ-LN25VG2R-ER3	
MSZ-LN25VG2R-ET2	
MSZ-LN25VG2R-ET3	
MSZ-LN25VG2R-SC1	
MSZ-LN25VG2V-E2	
MSZ-LN25VG2V-E3	
MSZ-LN25VG2V-EN2	
MSZ-LN25VG2V-ER2	
MSZ-LN25VG2V-ER3	
MSZ-LN25VG2V-ET2	
MSZ-LN25VG2V-ET3	
MSZ-LN25VG2V-SC1	
MSZ-LN25VG2W-E2	
MSZ-LN25VG2W-E3	
MSZ-LN25VG2W-EN2	
MSZ-LN25VG2W-ER2	
MSZ-LN25VG2W-ER3	
MSZ-LN25VG2W-ET2	
MSZ-LN25VG2W-ET3	
MSZ-LN25VG2W-SC1	
MSZ-LN35VG2B-E2	
MSZ-LN35VG2B-E3	
MSZ-LN35VG2B-EN2	
MSZ-LN35VG2B-ER2	
MSZ-LN35VG2B-ER3	
MSZ-LN35VG2B-ET2	
MSZ-LN35VG2B-ET3	
MSZ-LN35VG2B-SC1	
MSZ-LN35VG2R-E2	
MSZ-LN35VG2R-E3	
MSZ-LN35VG2R-EN2	
MSZ-LN35VG2R-ER2	
MSZ-LN35VG2R-ER3	
MSZ-LN35VG2R-ET2	
MSZ-LN35VG2R-ET3	
MSZ-LN35VG2R-SC1	
MSZ-LN35VG2V-E2	
MSZ-LN35VG2V-E3	
MSZ-LN35VG2V-EN2	
MSZ-LN35VG2V-ER2	
MSZ-LN35VG2V-ER3	
MSZ-LN35VG2V-ET2	
MSZ-LN35VG2V-ET3	
MSZ-LN35VG2V-SC1	
MSZ-LN35VG2W-E2	
MSZ-LN35VG2W-E3	
MSZ-LN35VG2W-EN2	
MSZ-LN35VG2W-ER2	
MSZ-LN35VG2W-ER3	

MSZ-LN35VG2W-ET2	
MSZ-LN35VG2W-ET3	
MSZ-LN35VG2W-SC1	
MSZ-LN50VG2B-E2	
MSZ-LN50VG2B-E3	
MSZ-LN50VG2B-EN2	
MSZ-LN50VG2B-ER2	
MSZ-LN50VG2B-ER3	
MSZ-LN50VG2B-ET2	
MSZ-LN50VG2B-ET3	
MSZ-LN50VG2B-SC1	
MSZ-LN50VG2R-E2	
MSZ-LN50VG2R-E3	
MSZ-LN50VG2R-EN2	
MSZ-LN50VG2R-ER2	
MSZ-LN50VG2R-ER3	
MSZ-LN50VG2R-ET2	
MSZ-LN50VG2R-ET3	
MSZ-LN50VG2R-SC1	
MSZ-LN50VG2V-E2	
MSZ-LN50VG2V-E3	
MSZ-LN50VG2V-EN2	
MSZ-LN50VG2V-ER2	
MSZ-LN50VG2V-ER3	
MSZ-LN50VG2V-ET2	
MSZ-LN50VG2V-ET3	
MSZ-LN50VG2V-SC1	
MSZ-LN50VG2W-E2	
MSZ-LN50VG2W-E3	
MSZ-LN50VG2W-EN2	
MSZ-LN50VG2W-ER2	
MSZ-LN50VG2W-ER3	
MSZ-LN50VG2W-ET2	
MSZ-LN50VG2W-ET3	
MSZ-LN50VG2W-SC1	
MSZ-LN60VG2B-E2	
MSZ-LN60VG2B-E3	
MSZ-LN60VG2B-ER2	
MSZ-LN60VG2B-ER3	
MSZ-LN60VG2B-ET2	
MSZ-LN60VG2B-ET3	
MSZ-LN60VG2R-E2	
MSZ-LN60VG2R-E3	
MSZ-LN60VG2R-ER2	
MSZ-LN60VG2R-ER3	
MSZ-LN60VG2R-ET2	
MSZ-LN60VG2R-ET3	
MSZ-LN60VG2V-E2	
MSZ-LN60VG2V-E3	
MSZ-LN60VG2V-ER2	
MSZ-LN60VG2V-ER3	
MSZ-LN60VG2V-ET2	
MSZ-LN60VG2V-ET3	
MSZ-LN60VG2W-E2	
MSZ-LN60VG2W-E3	
MSZ-LN60VG2W-ER2	
MSZ-LN60VG2W-ER3	
MSZ-LN60VG2W-ET2	
MSZ-LN60VG2W-ET3	
MSZ-RW25VG-E1	
MSZ-RW25VG-ER1	
MSZ-RW25VG-ET1	
MSZ-RW25VG-SC1	
MSZ-RW35VG-E1	
MSZ-RW35VG-ER1	



MSZ-RW35VG-ET1	
MSZ-RW35VG-SC1	
MSZ-RW50VG-E1	
MSZ-RW50VG-ER1	
MSZ-RW50VG-ET1	
MSZ-RW50VG-SC1	
MSZ-EF22VGKW-A1	
MSZ-EF22VGKB-A1	
MSZ-EF22VGKS-A1	
MSZ-EF25VGKW-A1	
MSZ-EF25VGKB-A1	
MSZ-EF25VGKS-A1	
MSZ-EF35VGKW-A1	
MSZ-EF35VGKB-A1	
MSZ-EF35VGKS-A1	
MSZ-EF42VGKW-A1	
MSZ-EF42VGKB-A1	
MSZ-EF42VGKS-A1	
MSZ-EF50VGKW-A1	
MSZ-EF50VGKB-A1	
MSZ-EF50VGKS-A1	
MSZ-AP22VGKD-A2	
MSZ-AP25VGKD-A2	
MSZ-AP35VGKD-A2	
MSZ-AP42VGKD-A2	
MSZ-AP50VGKD-A2	
MSZ-AP60VGKD-A2	
MSZ-AP71VGKD-A2	
MSZ-AP80VGKD-A2	
MSZ-LN25VG2V-A2	
MSZ-LN25VG2B-A2	
MSZ-LN25VG2R-A2	
MSZ-LN35VG2V-A2	
MSZ-LN35VG2B-A2	
MSZ-LN35VG2R-A2	
MSZ-LN50VG2V-A2	
MSZ-LN50VG2B-A2	
MSZ-LN50VG2R-A2	
MSZ-LN60VG2V-A2	
MSZ-LN60VG2B-A2	
MSZ-LN60VG2R-A2	
MSZ-AP60VGKD-A1	
MSZ-AP71VGKD-A1	
MSZ-AP80VGKD-A1	
MSZ-AP22VGKD-A1	
MSZ-AP25VGKD-A1	
MSZ-AP35VGKD-A1	
MSZ-AP42VGKD-A1	
MSZ-AP50VGKD-A1	
MSZ-AP60VGKD-A3	
MSZ-AP71VGKD2-A1	
MSZ-AP80VGKD2-A1	
MSZ-AP25VGKD2-A1	
MSZ-AP35VGKD-A3	
MSZ-AP42VGKD-A3	
MSZ-AP50VGKD-A3	
MSZ-LN25VG2B-A3	
MSZ-LN25VG2R-A3	
MSZ-LN25VG2V-A3	
MSZ-LN35VG2B-A3	
MSZ-LN35VG2R-A3	
MSZ-LN35VG2V-A3	
MSZ-LN50VG3B-A1	
MSZ-LN50VG3R-A1	
MSZ-LN50VG3V-A1	

MSZ-LN60VG3B-A1 MSZ-LN60VG3R-A1 MSZ-LN60VG3V-A1 MSZ-WX18VFK MSZ-WX20VFK MSZ-WX25VFK MSZ-ZY09VFK MSZ-ZY12VFK MSZ-ZY18VFK MSZ-GZY09VFK MSZ-GZY12VFK MSZ-GZY18VFK MSZ-KY09VFK MSZ-KY12VFK MSZ-KY18VFK MSZ-EZA09VAK MSZ-EZA12VAK MSZ-EXA09VAK MSZ-EXA12VAK MFZ-XT50VFK MFZ-XT60VFK MFZ-XT73VFK MFZ-GXT50VFK MFZ-GXT60VFK MFZ-GXT73VFK  Versions 36.00 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
MA-EW85S-E MA-EW85S-UK  Versions 80.00 and prior of the above models are affected.	<Impact> If the product receives data specially crafted by a malicious attacker within range of Wi-Fi communication, Wi-Fi communication of the product operating in access point mode may temporarily result in a DoS condition and suspend. As a result, device registration may become impossible.  <Countermeasures> Please carry out the mitigations below.  <Mitigations/Workarounds> Make sure that the SSID and KEY of the access point mode of the affected product are not known to an unspecified third party.  When using a PC, tablet or other device at home, please check the following. <ul style="list-style-type: none"> <li>- Please update your OS, software, anti-virus software, etc. to the latest version before use.</li> <li>- Do not open attachments or hyperlinks from unreliable sources or of unknown origin.</li> </ul>

\*Contact information

Please contact your local Mitsubishi Electric representative.

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