Denial of Service(DoS) and Remote Code Execution vulnerability in Amazon FreeRTOS memory allocation process

Release date: September 2, 2021
Mitsubishi Electric Corporation

■Overview

There is Denial of Service(DoS) and Remote Code Execution vulnerability due to a lack of memory size verification in Amazon RTOS memory allocation process (CVE-2021-31571). This vulnerability is one of a series of vulnerabilities called “Bad Allock”. This vulnerability could allow a malicious attacker to cause a denial of service (DoS) condition or remotely execute arbitrary code on a target product by providing specially crafted data. The following are the names of products affected by this vulnerability, please take mitigations.

■CVSS

CVE-2021-31571 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score:7.7

■Description

In the memory allocation process, it is necessary to verify that the requested memory size is within a certain range and that the calculation process is performed correctly. However, a vulnerability (CVE-2021-31571) has been found in Amazon FreeRTOS due to the lack of the validations in memory allocation process. The lack of the validations could causes an integer overflow (CWE-190). Our products may also be affected by this vulnerability.

■Impact

An attacker could cause an integer overflow to cause a denial of service (DoS) condition or remotely execute arbitrary code by providing specially crafted data to the target.

■Affected products, countermeasures, and mitigations or workarounds

[Wi-Fi Interface and Air Conditioning]

Model	Countermeasures and Mitigations/Workarounds
Wi-Fi Interface: S-MAC-002IF Air Conditioning: MFZ-GXT50/60/73VFK MFZ-XT50/60/73VFK MSZ-GZY09/12/18VFK MSZ-KY09/12/18VFK MSZ-WX18/20/25VFK MSZ-ZY09/12/18VFK MSZ-AP15/20/25/35/42/50VGK-E1 MSZ-AP15/20/25/35/42/50VGK-ER1 MSZ-AP15/20/25/35/42/50VGK-ET1 MSZ-AP25/35/42/50VGK-EN1 MSZ-AP15/20/25/35/42/50/60/71VGK-E2 MSZ-AP15/20/25/35/42/50/60/71VGK-ER2 MSZ-AP15/20/25/35/42/50/60/71VGK-ET2 MSZ-AP25/35/42/50VGK-EN2 MSZ-AP25/35/42/50/60/71VGK-E3 MSZ-AP25/35/42/50/60/71VGK-ER3 MSZ-AP25/35/42/50/60/71VGK-ET3 MSZ-AP25/35/42/50VGK-EN3 MSZ-AP25/35/42/50VGK-E7 MSZ-AP25/35/42/50VGK-E8 MSZ-BT20/25/35/50VGK-E1 MSZ-BT20/25/35/50VGK-E2 MSZ-BT20/25/35/50VGK-ET1 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-LN18/25/35/50/60VG2W(B)(R)(V)-E2 MSZ-LN25/35/50/60VG2W(B)(R)(V)-ER2 MSZ-LN25/35/50/60VG2W(B)(R)(V)-ET2 MSZ-LN25/35/50VG2W(B)(R)(V)-EN2 MSZ-RW25/35/50VG-E1 MSZ-RW25/35/50VG-ER1 MSZ-RW25/35/50VG-ET1 MSZ-RW25/35/50VG-SC1 MSZ-EF22/25/35/42/50VGKW(S)(B)-A1 MSZ-LN25/35/50/60VG2V(R)(B)-A2 The above models of version 3300 or less. “Version” is printed on Wi-Fi interface.	<Countermeasures> Please carry out 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.

<Inquiries>

https://www.mitsubishielectric.com/en/contact/room-air-conditioners.page