Arbitrary Code Execution Vulnerability in TCP Protocol Stack of Multiple Products

Release date: March 25, 2021
Mitsubishi Electric Corporation

■Overview

There is a vulnerability in the Treck TCP/IP stack of multiple our products. If this vulnerability is exploited by a malicious attacker, there are risks such as denial of service (DoS) and remote code execution (RCE). (CVE-2020-25066)
The following are the names of products affected by this vulnerability, please take workarounds.

■CVSS

CVE-2020-25066: CVSS 3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H Base Score:9.0

■Affected products

All versions of the following Wi-Fi Interfaces

1) MAC-557IF-E
2) MAC-558IF-E
3) MAC-559IF-E
4) PAC-WF010-E
5) PAC-WHS01WF-E

■Description

Treck TCP/IP Stack in our products has a heap-based buffer overflow (CWE-122) caused by improper bounds checking by the HTTP Server component, when HTTP Server component is enabled. This vulnerability allows malicious attackers to cause denial of service (DoS) or remote code execution (RCE).

■Impact

A malicious attacker may cause denial of service (DoS) or remote code execution (RCE) by abusing this vulnerability.

■Countermeasures

Mitsubishi Electric recommends to implement following workarounds.

■Workarounds

1.Check if the Wi-Fi router settings are as follows.

1-1. Set wireless LAN encryption key that is hard to 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 Wi-Fi router settings, hide its presence on the internet in order to make unauthorized access difficult. (e.g. Set to not respond to PING request)
1-4. Set password for the Wi-Fi 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 OS, Antivirus software, etc. 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