Impact of Multiple Vulnerabilities in TCP/IP Stack (Ripple 20)

Release date: September 24, 2020
Mitsubishi Electric Corporation

Overview

19 vulnerabilities in TCP/IP Stack (Ripple20) have been disclosed. If these vulnerabilities are exploited by a malicious attacker, there are several risks such as information disclosure, information destruction or tampering, denial of service (DoS), and remote code execution (RCE). Some of these vulnerabilities affect several our products.

The following are the names of products affected by some of these vulnerabilities, please take countermeasures or mitigations/workarounds. And the names of products affected by some of these vulnerabilities as well as countermeasures and mitigations/workarounds will be updated one by one.

Description

In Treck IP Stack and Zuken Elmic IP Stack (KASAGO ®) there are 19 vulnerabilities listed below. And our products may also be affected by some of them. **Please check the vulnerability numbers (1 – 19 below) that may affect each product in "Affected products, countermeasures, and mitigations or workarounds".**

(1) Remote Code Execution vulnerability in IPv4 and UDP components (CVE-2020-11896)
(2) Remote Code Execution vulnerability in IPv6 component (CVE-2020-11897)
(3) Information Disclosure vulnerability in IPv4 and ICMPv4 components (CVE-2020-11898)
(4) Information Disclosure and Denial of Service (DoS) vulnerabilities in IPv6 component (CVE-2020-11899)
(5) Denial of Service (DoS) vulnerability in IPv4 tunneling component (CVE-2020-11900)
(6) Remote Code Execution vulnerability in DNS resolver component (CVE-2020-11901)
(7) Information Disclosure vulnerability in IPv6 over IPv4 tunneling component (CVE -2020 -11902)
(8) Information Disclosure vulnerability in DHCP component (CVE-2020-11903)
(9) Information Corruption, Denial of Service (DoS), and Remote Code Execution vulnerabilities in Memory Allocation component (CVE-2020-11904)
(10) Information Disclosure vulnerability in DHCPv6 Component (CVE-2020-11905)
(11) Denial of Service (DoS) vulnerability in Ethernet Link Layer component (CVE-2020-11906)
(12) Denial of Service (DoS) vulnerability in TCP components (CVE-2020-11907)
(13) Information Disclosure vulnerability in DHCP component (CVE-2020-11908)
(14) Denial of Service (DoS) vulnerability in IPv4 component (CVE-2020-11909)
(15) Information Disclosure vulnerability in ICMPv4 component (CVE-2020-11910)
(16) Denial of Service (DoS) vulnerability in ICMPv4 component (CVE-2020-11911)
(17) Information Disclosure vulnerability in TCP component (CVE-2020-11912)
(18) Information Disclosure vulnerability in IPv6 component (CVE-2020-11913)
(19) Information Disclosure vulnerability in ARP component (CVE-2020-11914)

Impact

The expected threats vary from product to product, but if these vulnerabilities are exploited by an attacker, there are several impacts such as information disclosure, information destruction or tampering, denial of service (DoS), and remote code execution (RCE).

Affected products, countermeasures, and mitigations or workarounds

[1] [Wi-Fi Interface]

Model	Countermeasures and Mitigations/Workarounds
MAC-557IF-E PAC-WF010-E MAC-558IF-E MAC-559IF-E PAC-WHS01WF-E (Could be affected by 3, 6, 9, 12, 13, 16,17, 19)	<Expected Impact> If these vulnerabilities are exploited by a malicious attacker, there may be several impacts such as denial of service (DoS), information tampering, or information disclosure. <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.

References

- CERT/CC Vulnerability Note "VU#257161 Treck IP stacks contain multiple vulnerabilities"
  https://www.kb.cert.org/vuls/id/257161
- ICS Advisory "ICSA-20-168-01 Treck TCP/IP Stack"
  https://www.us-cert.gov/ics/advisories/icsa-20-168-01
- JSOF "Ripple20"
  https://www.jsof-tech.com/ripple20/
- Treck Inc. "Vulnerability Response Information"
  https://treck.com/vulnerability-response-information/