Information Disclosure Vulnerability and Denial-of-Service (DoS) Vulnerability due to OpenSSL Vulnerabilities in CC-Link IE TSN Industrial Managed Switch

Release date: October 05, 2023
Last update date: June 04, 2024
Mitsubishi Electric Corporation

Overview

Information disclosure vulnerability and Denial-of-Service (DoS) vulnerability due to OpenSSL vulnerabilities exist in CC-Link IE TSN Industrial Managed Switch. An attacker could disclose information stored in the product by sending specially crafted packets or could cause denial-of service (DoS) condition by getting a legitimate user to import specially crafted certificate. (CVE-2022-4304, CVE-2022-4450)

CVSS[1]

CVE-2022-4304	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score:5.9
CVE-2022-4450	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	Base Score:6.5

Affected products

Affected products and firmware versions are below.

No	Product Name	Model Name	Affected firmware version
1	CC-Link IE TSN Industrial Managed Switch	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	”05” and prior

[How to check the version in use]

(1) After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 through the web interface, [Device Summary] screen is displayed.
(2) Confirm the first 2 characters (digits) of the strings in Firmware Version on Model Information displayed in [Device Summary] screen (see Figure 1)
ex) When “02 Build xxxx” is displayed, its firmware version is “02”.

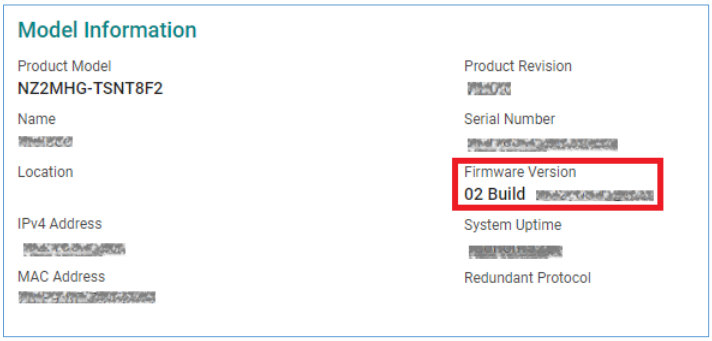

Figure 1 NZ2MHG-TSNT8F2 Model Information view

Description

The following two vulnerabilities exist in CC-Link IE TSN Industrial Managed Switches.

・CVE-2022-4304 : An information disclosure vulnerability due to Observable Timing Discrepancy (CWE-208[2]) in RSA decryption implementations.

・CVE-2022-4450 : A Denial-of-Service (DoS) vulnerability due to Double Free (CWE-415[3]) when reading a PEM file.

Impact

By sending specially crafted packets and performing a Bleichenbacher style attack (*1), an attacker could decrypt the ciphertext and disclose sensitive information (CVE-2022-4304). Or an attacker could cause denial-of-service (DoS) on the product by leading a legitimate user to import a malicious certificate (CVE-2022-4450).
*1: An attack method to decrypt ciphertext by observing the behavior when a padding error occurs

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/208.html
3 https://cwe.mitre.org/data/definitions/415.html

Countermeasures

Please update to the fixed versions by following the steps below.

[Fixed versions]

No.	Product Name	Model Name	Fixed software/firmware version
1	CC-Link IE TSN Industrial Managed Switch	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	“06” or later

[Update steps]

(1) Please contact your local Mitsubishi Electric representative to obtain the fixed firmware version file for CC-Link IE TSN Industrial Managed Switch.

(2) After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 through the web interface, please update the firmware to the fixed firmware version file mentioned in the above (1) by the function of [System] -> [System Management] -> [Firmware Upgrade] from Function menu.
For the detailed procedures, please refer to "CC-Link IE TSN Industrial Managed Switch User's Manual (SH-082449ENG)".

(3) Refer to the <How to check the version in use> to check that the firmware has been updated to the fixed version.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting these vulnerabilities:

・When Internet access is required, use a virtual private network (VPN) or other means to prevent unauthorized access.

・Use the products within a LAN and block access from untrusted networks and hosts.

・Restrict physical access to your computer and network equipment on the same network.

・After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 with the web interface, change user name and password from default setting at [Account Management] displayed on the function menu. Also, set the proper access permissions for the users.

Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html

Update history

June 04, 2024
Added the affected firmware version and [How to check the version in use] to “Affected products”.
Added the fixed firmware version and [Update steps] to “Countermeasures”.