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

Release date: June 04, 2024
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability due to OpenSSL vulnerability exists in CC-Link IE TSN Industrial Managed Switch. An attacker could cause temporary denial-of service (DoS) condition in web service on the product by getting a legitimate user to import specially crafted certificate that makes the product experience notable to very long delays. However, administrator privilege is required to import certificate. (CVE-2023-2650)

CVSS[1]

CVE-2023-2650 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L Base Score:2.7

Affected products

Affected products and firmware versions are below.

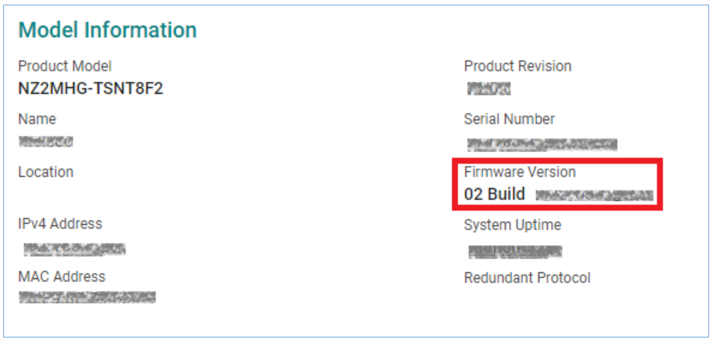
No	Product Name	Model Name	Affected firmware version
1	CC-Link IE TSN Industrial Managed Switch	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	”05” and prior

[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”.



Model Information

Product Model
NZ2MHG-TSNT8F2

Name
[redacted]

Location

IPv4 Address
[redacted]

MAC Address
[redacted]

Product Revision
[redacted]

Serial Number
[redacted]

Firmware Version
02 Build [redacted]

System Uptime
[redacted]

Redundant Protocol

Figure 1 NZ2MHG-TSNT8F2 Model Information view

Description

A denial-of-service (DoS) vulnerability (CVE-2023-2650) due to Allocation of Resources Without Limits or Throttling (CWE-770[2]) exists in OpenSSL installed on CC-Link IE TSN Industrial Managed Switches.

Impact

An attacker could cause temporary denial-of-service (DoS) condition in web service on the product by getting a legitimate user to import specially crafted certificate that makes the product experience notable to very long delays. However, administrator privilege is required to import certificate.

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/770.html

Countermeasures

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

[Fixed versions]

No.	Product Name	Model Name	Fixed 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 this vulnerability:

- 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 the product and your computer and network equipment on the same network.
- After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 through 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