Authentication Bypass Vulnerability in MELSEC WS Series Ethernet Interface Module

Release date: May 18, 2023
Last update date: August 22, 2023
Mitsubishi Electric Corporation

■Overview

Authentication bypass vulnerability exists in MELSEC WS Ethernet Interface Module.

A remote unauthenticated attacker may bypass authentication and log in illegally by connecting to the module via Telnet. As a result, a remote attacker with unauthorized login can reset the module, and if certain conditions are met, he/she can disclose or tamper with the module's configuration, or rewrite the firmware.(CVE-2023-1618).

■CVSS[1]

CVE-2023-1618 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:7.5

■Affected products

Affected products and serial number are below.

Series	Product Name	Serial number
MELSEC WS Series	WS0-GETH00200	Serial number are "2310 ****" and prior

The serial number can be found on the type label and on the Hardware configuration screen of the online status Setting and Monitoring Tool.

■Description

In the affected products, the hidden Telnet function is enabled by default when shipped from the factory (CWE-489)[2], so that an authentication bypass vulnerability allows a remote unauthenticated attacker to illegally log into the affected module by connecting to it via telnet.

■Impact

A remote unauthenticated attacker may bypass authentication and log in illegally by connecting to the module via Telnet. As a result, an attacker who logs in illegally can reset the module, and if certain conditions are met, he/she can disclose or tamper with the module's configuration, or rewrite the firmware.

■Countermeasures

We have fixed the vulnerability at the following serial number.

Series	Product Name	Serial number
MELSEC WS Series	WS0-GETH00200	Serial number are "2311 ****" or later

If you have affected products, please take the following Mitigations/Workarounds.

■Mitigations/Workarounds

Set password for telnet sessions that are difficult for third parties to guess. The password can be up to 15 characters long.

You can change the password for the Telnet session of the affected product by using the Telnet client and performing the following (1) to (2). Note that "[space]" in the input string represents a single-byte space.

(1) Password setting
1) Enter "telnet[space]" followed by the IP address of the affected product and press the Enter key.
2) When "Password" is displayed, press the Enter key without entering anything.
3) When "telnet>" is displayed, enter "password[space]" followed by the password string you want to set and press the Enter key.
4) Finally, enter "quit" and press the Enter key.

(2) Confirm that the password is set
1) After performing (1), enter "telnet[space]" followed by the IP address of the affected product and press the Enter key.
2) When "Password" is displayed, enter the password string set in (1) and press the Enter key.
3) If "telnet>" is displayed, the password is set correctly.
4) Finally, enter "quit" and press the Enter key.

Alternatively, Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to prevent untrusted devices from connecting to the LAN.

---

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

2 https://cwe.mitre.org/data/definitions/489.html

■Contact information

Please contact your local Mitsubishi Electric representative.

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

■Update history

August 22, 2023

Added a serial number that have been fixed to “Countermeasures”