Authentication Bypass Vulnerability in MELSEC WS Series Ethernet Interface Module

Release date: January 30, 2024
Mitsubishi Electric Corporation

Overview

An authentication bypass vulnerability exists in the MELSEC WS Series Ethernet Interface Modules. A remote unauthenticated attacker can bypass authentication by capture-replay attack*1 and illegally login to the modules. As a result, the remote attacker who has logged in illegally may be able to disclose or tamper with the programs and parameters in the modules. (CVE-2023-6374)

*1 : An attack in which an attacker captures login information that flows through the network when a legitimate user logs in by sniffing, and attempts to log in illegally by replaying the obtained login information.

CVSS[1]

CVE-2023-6374 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score 5.9

Affected products

The following products and serial numbers are affected:

Series	Product name	Serial number
MELSEC WS Series	WS0-GETH00200	All serial numbers

Description

An authentication bypass vulnerability due to Authentication Bypass by Capture-replay (CWE-294[2]) exists in the MELSEC WS Series Ethernet Interface Modules.

Impact

A remote unauthenticated attacker can bypass authentication by capture-replay attack and illegally login to the modules. As a result, the remote attacker who has logged in illegally may be able to disclose or tamper with the programs and parameters in the modules.

Countermeasures

Please carry out mitigations/workarounds.

Mitigations / Workarounds

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

- Use a virtual private network (VPN), etc. to encrypt the communication between affected products and the peer.
- Use a firewall or 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 affected products and to personal computers and network devices located in the LAN to which the affected products are connected.

Contact information

Please contact your local Mitsubishi Electric representative.

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

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

[2] https://cwe.mitre.org/data/definitions/294.html