

# Authentication Bypass Vulnerability in Multiple Air Conditioning Systems

Release date: June 26, 2025  
Mitsubishi Electric Corporation

## Overview

Authentication bypass vulnerability exists in Mitsubishi Electric air conditioning systems. An attacker may bypass authentication and then control the air conditioning systems illegally, or disclose information in them by exploiting this vulnerability. In addition the attacker may tamper with firmware for the affected products using the disclosed information (CVE-2025-3699).

Mitsubishi Electric air conditioning systems are premised that they are used in intranet (networks inside a building) or in secure environments with VPN routers, etc. such as System Example 1 or 2 in section "Description". Please make sure that your system is configured correctly as recommended by Mitsubishi Electric.

## CVSS<sup>1</sup>

CVE-2025-3699 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score: 9.8

## Affected products

The affected products and versions are as follows.

<Models and Versions>

Model	Version
G-50	Ver.3.37 and prior
G-50-W	Ver.3.37 and prior
G-50A	Ver.3.37 and prior
GB-50	Ver.3.37 and prior
GB-50A	Ver.3.37 and prior
GB-24A	Ver.9.12 and prior
G-150AD	Ver.3.21 and prior
AG-150A-A	Ver.3.21 and prior
AG-150A-J	Ver.3.21 and prior
GB-50AD	Ver.3.21 and prior
GB-50ADA-A	Ver.3.21 and prior
GB-50ADA-J	Ver.3.21 and prior
EB-50GU-A	Ver.7.11 and prior
EB-50GU-J	Ver.7.11 and prior
AE-200J	Ver.8.01 and prior
AE-200A	Ver.8.01 and prior
AE-200E	Ver.8.01 and prior
AE-50J	Ver.8.01 and prior
AE-50A	Ver.8.01 and prior
AE-50E	Ver.8.01 and prior
EW-50J	Ver.8.01 and prior
EW-50A	Ver.8.01 and prior
EW-50E	Ver.8.01 and prior
TE-200A	Ver.8.01 and prior
TE-50A	Ver.8.01 and prior
TW-50A	Ver.8.01 and prior
CMS-RMD-J	Ver.1.40 and prior

<How to check the versions>

•G-50, G-50-W, G-50A, GB-50, GB-50A, GB-24A, G-150AD, AG-150A-A, AG-150A-J, GB-50AD, GB-50ADA-A, GB-50ADA-J, EB-50GU-A, EB-50GU-J, and CMS-RMD-J

By selecting [Registration of Optional Functions] on Login Page of their WEB screen, you can check the versions (see Figure 1).

---

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


**Figure 1 How to check the versions on G-50, G-50-W, G-50A, GB-50, GB-50A, GB-24A, G-150AD, AG-150A-A, AG-150A-J, GB-50AD, GB-50ADA-A, GB-50ADA-J, EB-50GU-A, EB-50GU-J, and CMS-RMD-J**

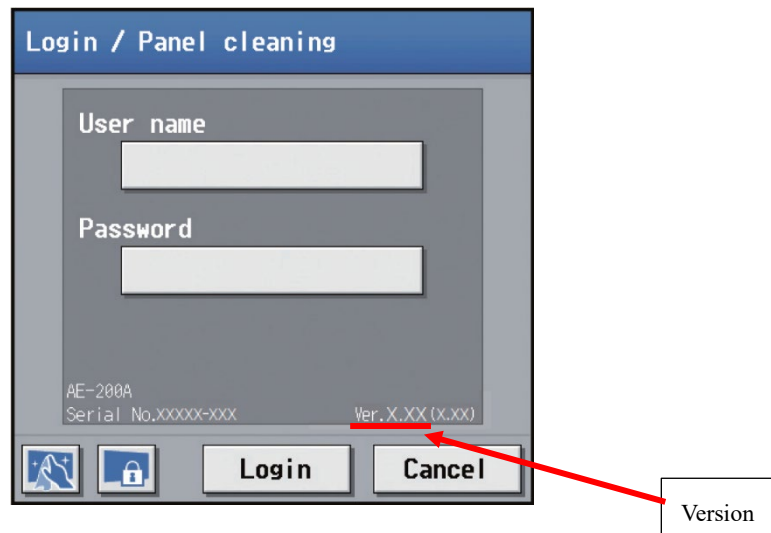
• AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, EW-50J, EW-50A, EW-50E, TE-200A, TE-50A, and TW-50A

By selecting [License Registration] on Setting tab in the home screens after you log in as administrators on their WEB screen, you can check the versions (see Figure 2).

**Figure 2 How to check the versions on AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, EW-50J, EW-50A, EW-50E, TE-200A, TE-50A, and TW-50A**

• Another way to check versions of G-150AD, AG-150A-A, AG-150A-J, AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, TE-200A, and TE-50A

By touching  on the upper right corner of the normal screens to display the login window, you can check the versions (see Figure 3).



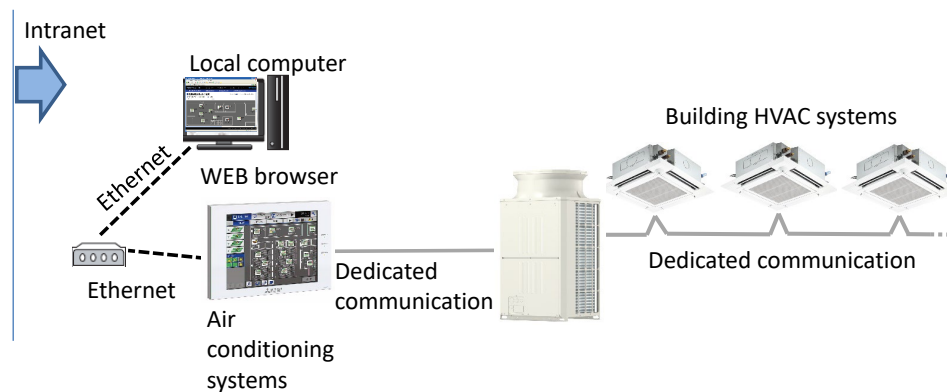
**Figure 3** Another way to check the versions on G-150AD, AG-150A-A, AG-150A-J, AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, TE-200A, and TE-50A

## Description

Authentication bypass vulnerability due to Missing Authentication for Critical Function (CWE-306<sup>2</sup>) exists in Mitsubishi Electric air conditioning systems.

In case of System Example 1 and 2, even if an attacker tries to exploit the vulnerabilities from internet, the attack will not succeed. In case of System Example 3, if an attacker tries to exploit the vulnerabilities from internet, the attack may succeed. Please make sure that your system is configured correctly as recommended by Mitsubishi Electric.

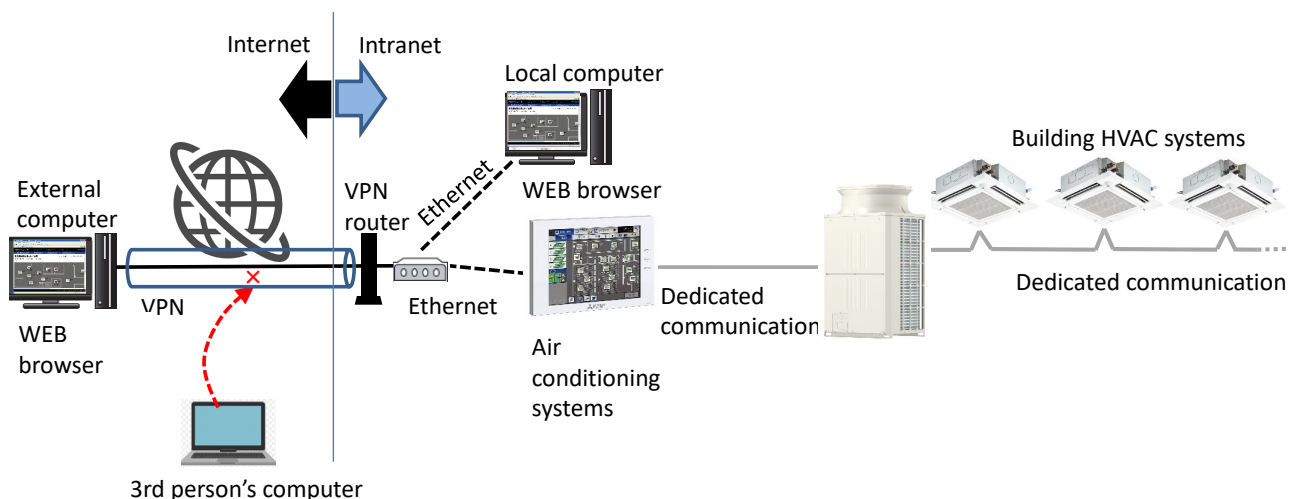
**System Example 1:** A configuration using air conditioning systems in intra networks (Figure 4)



**Figure 4** System Example 1

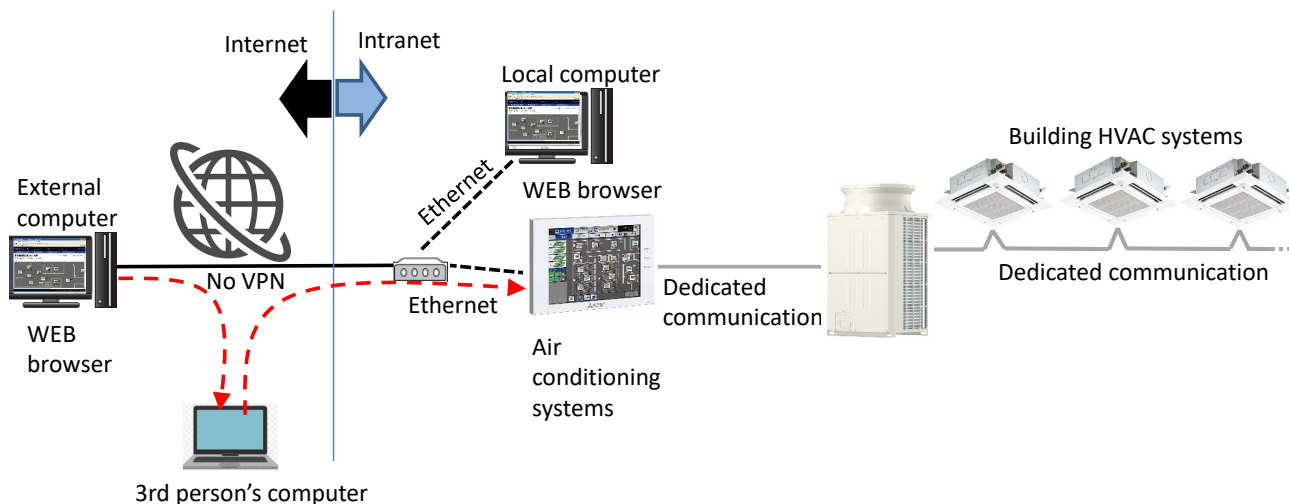
<sup>2</sup> <https://cwe.mitre.org/data/definitions/306.html>

**System Example 2:** A configuration using air conditioning systems which is accessible from external computers via a VPN router (Figure 5)



**Figure 5 System Example 2**

**System Example 3:** A configuration using air conditioning systems which is accessible from external computers without VPN (improper configuration, Figure 6)



**Figure 6 System Example 3**

## Impact

An attacker may bypass authentication and then control the systems illegally or disclose information in them. In addition the attacker may also tamper with the firmware for the affected products using the disclosed information.

## Countermeasures for Customers

There are no plans to release a fixed version, so please take the following Mitigations. Mitsubishi Electric is currently preparing improved versions for the following products to mitigate this vulnerability.

AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, EW-50J, EW-50A, EW-50E, TE-200A, TE-50A, and TW-50A

## **Mitigations**

To minimize the risk of this vulnerability being exploited, please make sure that your air conditioning system is configured correctly as recommended by Mitsubishi Electric. And Mitsubishi Electric recommends to take the following mitigation measures.

- Restrict the access to your air conditioning system from untrusted networks and hosts.
- Restrict physical access to your air conditioning system, your computer which can access to it, and the network which is connected to them.
- Use an anti-virus software and update the OS and the WEB browser to the latest version on your computer to connect your air conditioning system.

## **Acknowledgement**

Mitsubishi Electric would like to thank Mihály Csonka who reported these vulnerabilities.

## **Contact information**

Please contact your local Mitsubishi Electric representative.