

Privilege Escalation Vulnerability in WEB Functions of Air Conditioning Systems

Release date: July 1, 2021
Mitsubishi Electric Corporation

■ Overview

WEB functions of Mitsubishi Electric air conditioning systems have a privilege escalation vulnerability due to incorrect implementation of authentication algorithm (CWE-303). A malicious attacker may impersonate administrators to disclose configuration information of the air conditioning system and tamper information (e.g. operation information and configuration of air conditioning system) by exploiting this vulnerability (CVE-2021-20593).

■ CVSS

CVE-2021-20593 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:N Base score:7.1

■ Affected products

<Models and Versions>

【Air Conditioning System / Centralized Controllers】

| Model | Versions |
|------------|----------------------------|
| G-50A | From ver.2.50 to ver. 3.35 |
| GB-50A | From ver.2.50 to ver. 3.35 |
| AG-150A-A | Ver.3.20 and prior |
| AG-150A-J | Ver.3.20 and prior |
| GB-50ADA-A | Ver.3.20 and prior |
| GB-50ADA-J | Ver.3.20 and prior |
| EB-50GU-A | Ver 7.09 and prior |
| EB-50GU-J | Ver 7.09 and prior |
| AE-200A | Ver 7.93 and prior |
| AE-200E | Ver 7.93 and prior |
| AE-50A | Ver 7.93 and prior |
| AE-50E | Ver 7.93 and prior |
| EW-50A | Ver 7.93 and prior |
| EW-50E | Ver 7.93 and prior |
| TE-200A | Ver 7.93 and prior |
| TE-50A | Ver 7.93 and prior |
| TW-50A | Ver 7.93 and prior |
| CMS-RMD-J | Ver.1.30 and prior |

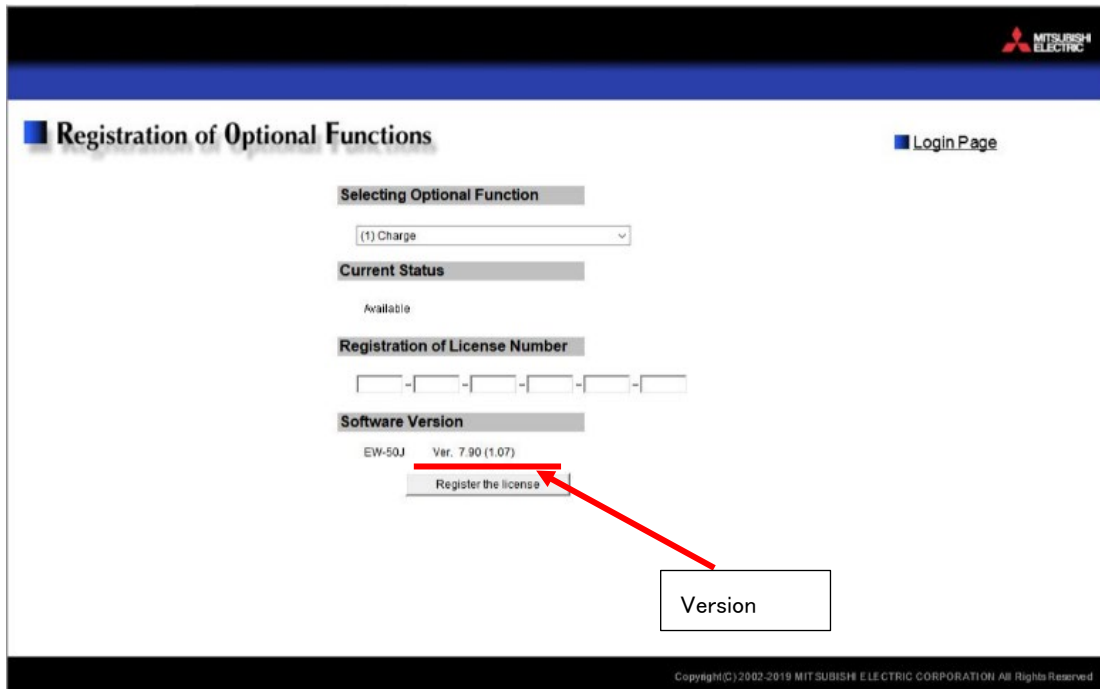
【Air Conditioning System /Expansion Controllers】

| Model | Versions |
|-------------|--------------------|
| PAC-YG50ECA | Ver.2.20 and prior |

<How to check the versions>

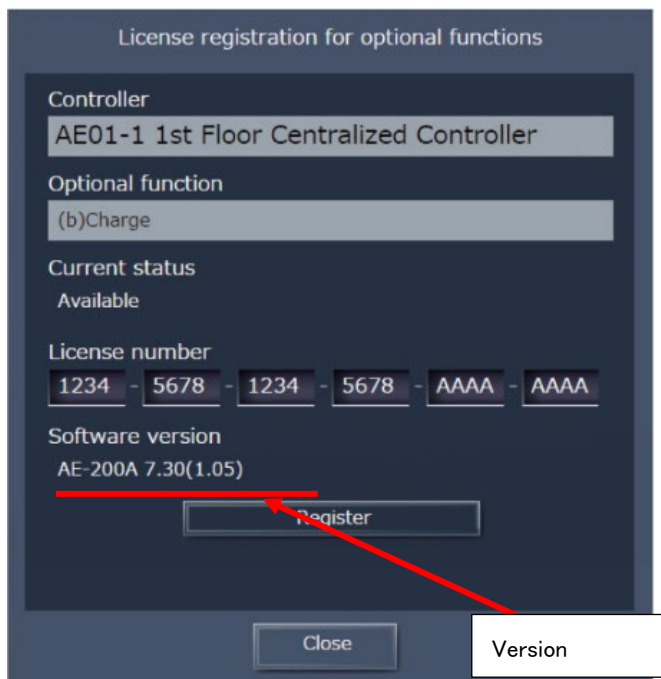
•G-50A, GB-50A, AG-150A-A, AG-150A-J, GB-50ADA-A, GB-50ADA-J, EB-50GU-A, EB-50GU-J, CMS-RMD-J, and PAC-YG50ECA

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




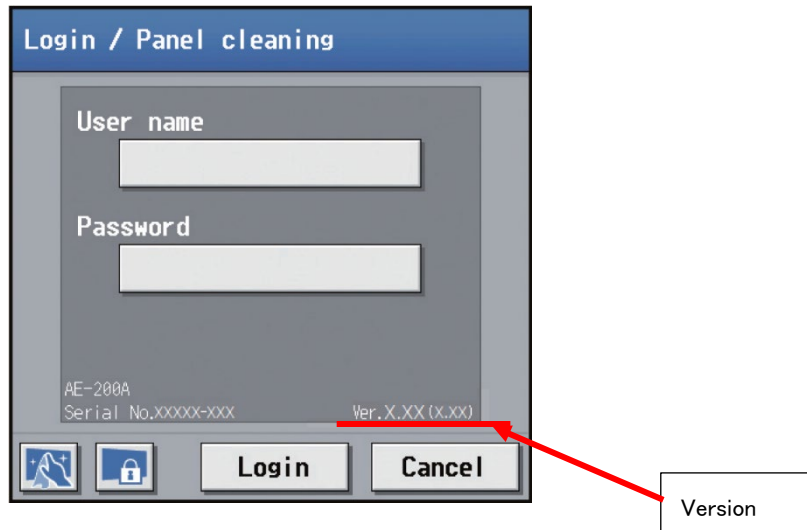
•AE-200A, AE-200E, AE-50A, AE-50E, EW-50A, EW-50E, TE-200A, TE-50A, and TW-50A

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



•How to check versions on the screens of AG-150A-A, AG-150A-J, AE-200A, AE-200E, 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.



■Description

WEB functions of our air conditioning systems have a privilege escalation vulnerability due to incorrect implementation of authentication algorithm (CWE-303).

■Impact

A malicious attacker may impersonate administrators to disclose configuration information of the air conditioning system and tamper information (e.g. operation information and configuration of air conditioning system) by exploiting this vulnerability.

■Countermeasures

The fixed firmware versions are as follows.

<Models and Versions>

【Air Conditioning System / Centralized Controllers】

| Model | Versions |
|------------|-------------------|
| G-50A | Ver.3.37 or later |
| GB-50A | Ver.3.37 or later |
| AG-150A-A | Ver.3.21 or later |
| AG-150A-J | Ver.3.21 or later |
| GB-50ADA-A | Ver.3.21 or later |
| GB-50ADA-J | Ver.3.21 or later |
| EB-50GU-A | Ver 7.10 or later |
| EB-50GU-J | Ver 7.10 or later |
| AE-200A | Ver 7.95 or later |
| AE-200E | Ver 7.95 or later |
| AE-50A | Ver 7.95 or later |
| AE-50E | Ver 7.95 or later |
| EW-50A | Ver 7.95 or later |
| EW-50E | Ver 7.95 or later |
| TE-200A | Ver 7.95 or later |
| TE-50A | Ver 7.95 or later |
| TW-50A | Ver 7.95 or later |
| CMS-RMD-J | Ver.1.40 or later |

【Air Conditioning System /Expansion Controllers】

| Model | Versions |
|-------------|-------------------|
| PAC-YG50ECA | Ver.2.21 or later |

<How to update>

Please contact the distributor or Mitsubishi Electric representative.

■ Mitigations

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

- Use a VPN router, etc. when you connect your air conditioning system to the Internet.
- Use an anti-virus software on your computer to connect your air conditioning system.
- Restrict the access to your air conditioning system from untrusted networks and hosts.
- Change default user names and passwords.

■ Acknowledgement

Mitsubishi Electric would like to thank Chizuru Toyama of TXOne IoT/ICS Security Research Labs working with Trend Micro's Zero Day Initiative who reported this vulnerability.

■ Contact information

Please contact your local Mitsubishi Electric representative.