Privilege Escalation Vulnerability in WEB Functions of Air Conditioning Systems

Release date: July 1, 2021
Last update date: September 16, 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).

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

■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

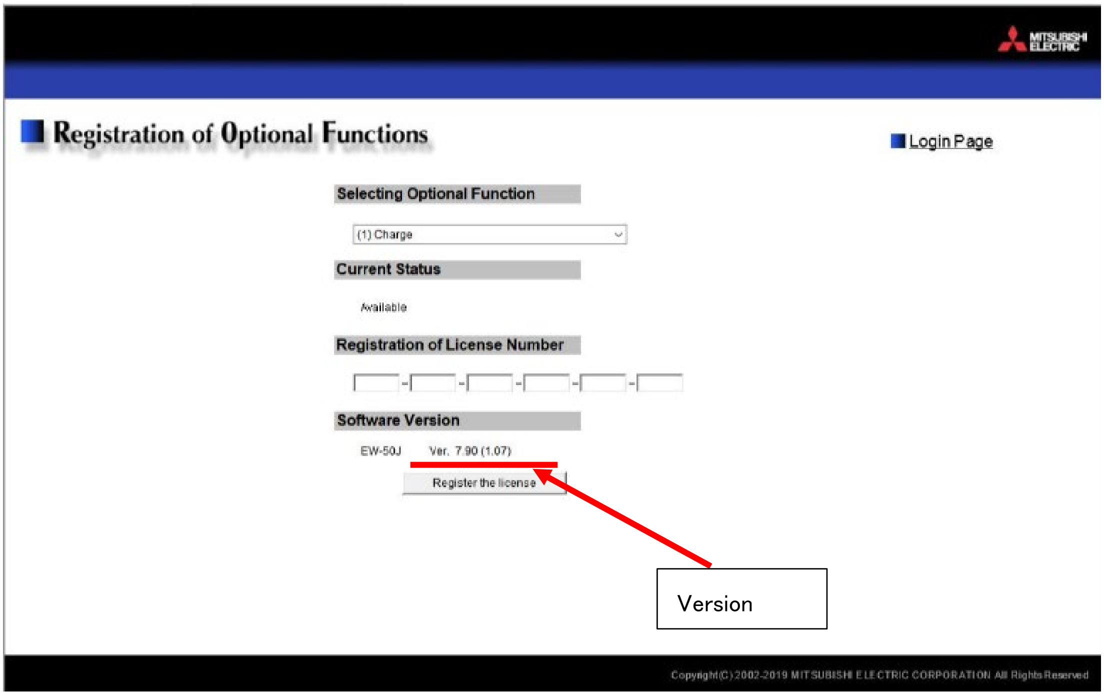
【Air Conditioning System /Expansion Controllers】

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.



Registration of Optional Functions

Selecting Optional Function

(1) Charge

Current Status

Available

Registration of License Number

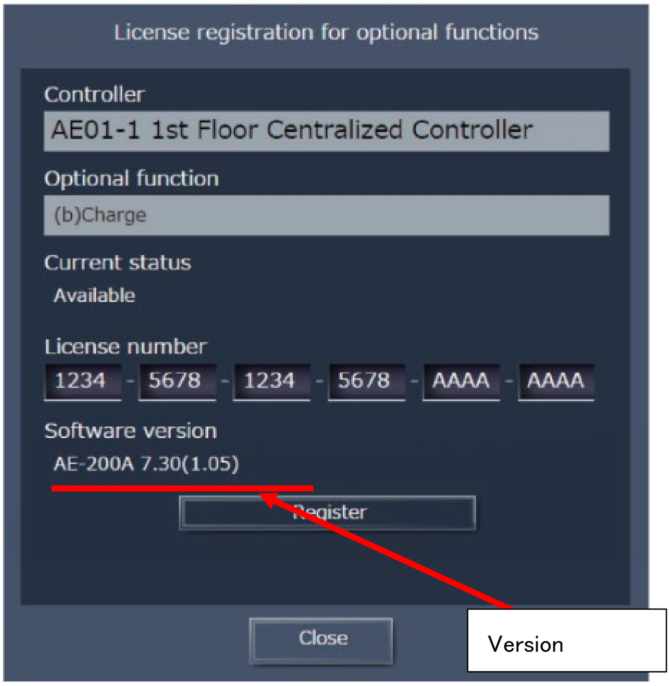
Software Version

EW-50J　Ver. 7.90 (1.07)

Login Page
Register the license
Version
Copyright(C)2002-2019 MITSUBISHI ELECTRIC CORPORATION All Rights Reserved

・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.



License registration for optional functions

Controller

AE01-1 1st Floor Centralized Controller

Optional function

(b)Charge

Current status

Available

License number

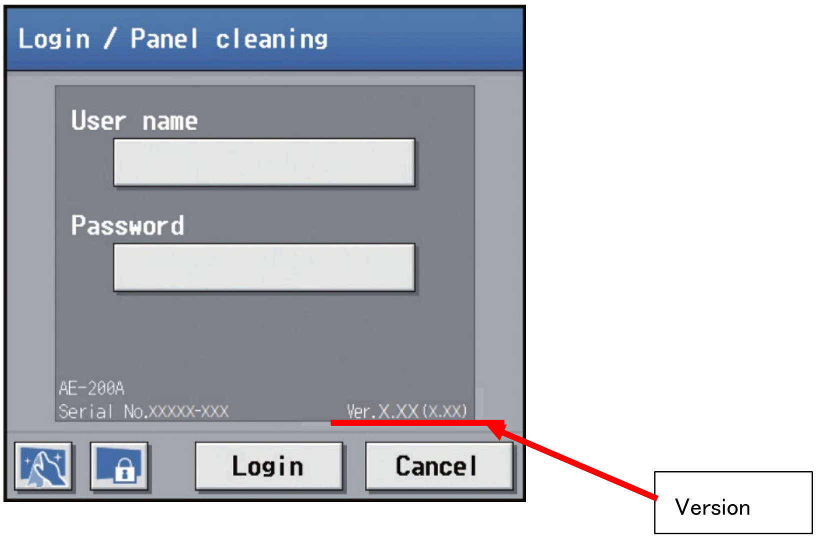
1234 - 5678 - 1234 - 5678 - AAAA - AAAA

Software version

AE-200A 7.30(1.05)

・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.



Login / Panel cleaning

User name

Password

AE-200A
Serial No.XXXXX-XXX Ver.X.XX(X.XX)

Version

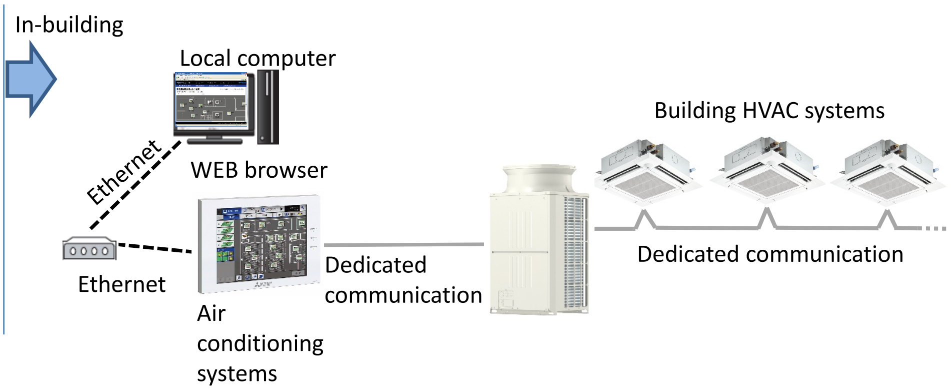
■Description

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

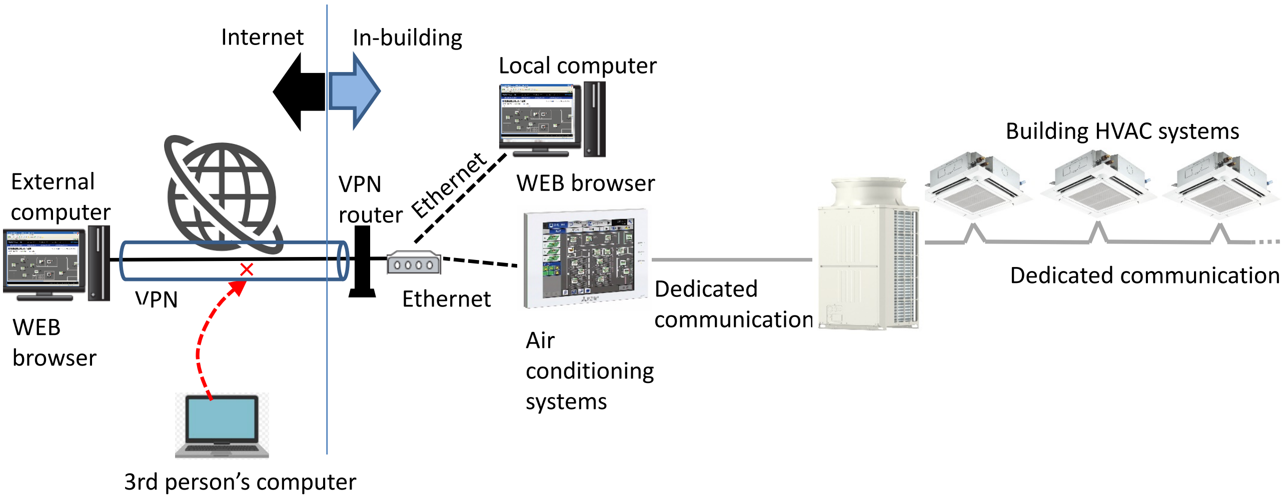
In case of System Example 1 and 2, even if an attacker tries to exploit the vulnerability from the Internet, the attack will not succeed.

In case of System Example 3, if an attacker tries to exploit the vulnerability from the Internet, the attack may succeed. Please make sure that your system is properly configured as recommended by Mitsubishi Electric.

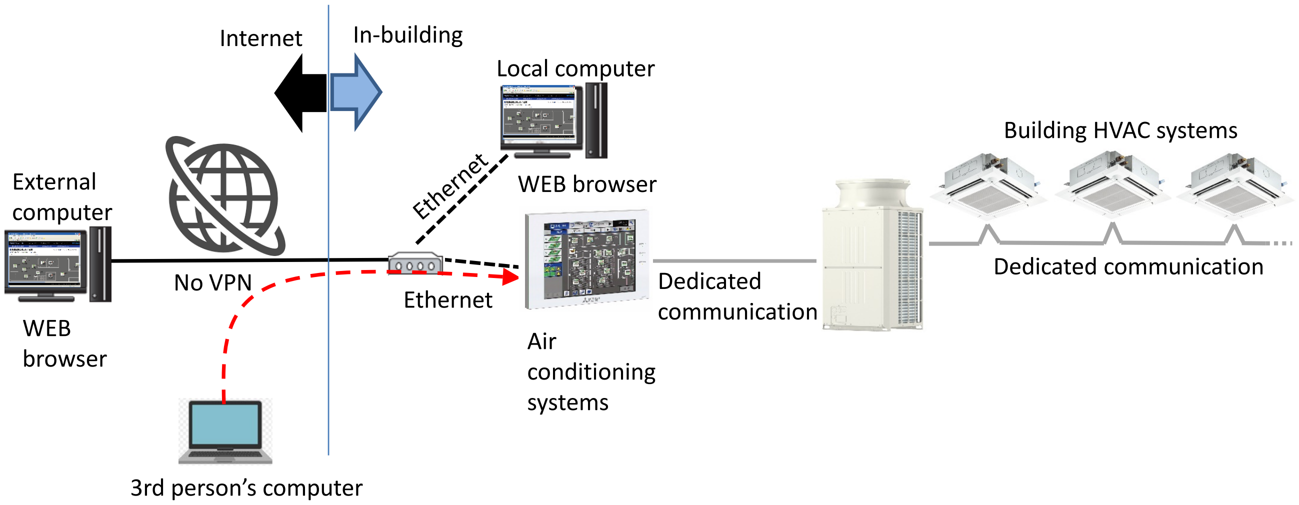
System Example 1: A configuration using air conditioning systems in in-building networks



System Example 2: A configuration using air conditioning systems which is accessible from exnternal computers via a VPN router



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



■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

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

・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.

■Update histroy

September 16, 2021
Added information to ″Overview″
Added System Examples to ″Description″
Modified ″Mitigations″