

Information Disclosure and Denial-of-Service Vulnerability in Multiple Air Conditioning Systems

Release date: July 1, 2021
Mitsubishi Electric Corporation

■ Overview

Mitsubishi Electric air conditioning systems have an information disclosure and Denial-of-Service (DoS) vulnerability due to improper restriction of XML external entity reference (XXE) (CVE-611). A malicious attacker may disclose some of data in the air conditioning system or cause DoS condition by sending a specially crafted packet (CVE-2021-20595).

■ CVSS

CVE-2021-20595 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H Base Score:9.3

■ Affected products

<Models and Versions>

【Air Conditioning System / Centralized Controllers】

Model	Versions
G-50A	Ver.3.35 and prior
GB-50A	Ver.3.35 and prior
GB-24A	Ver.9.11 and prior
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

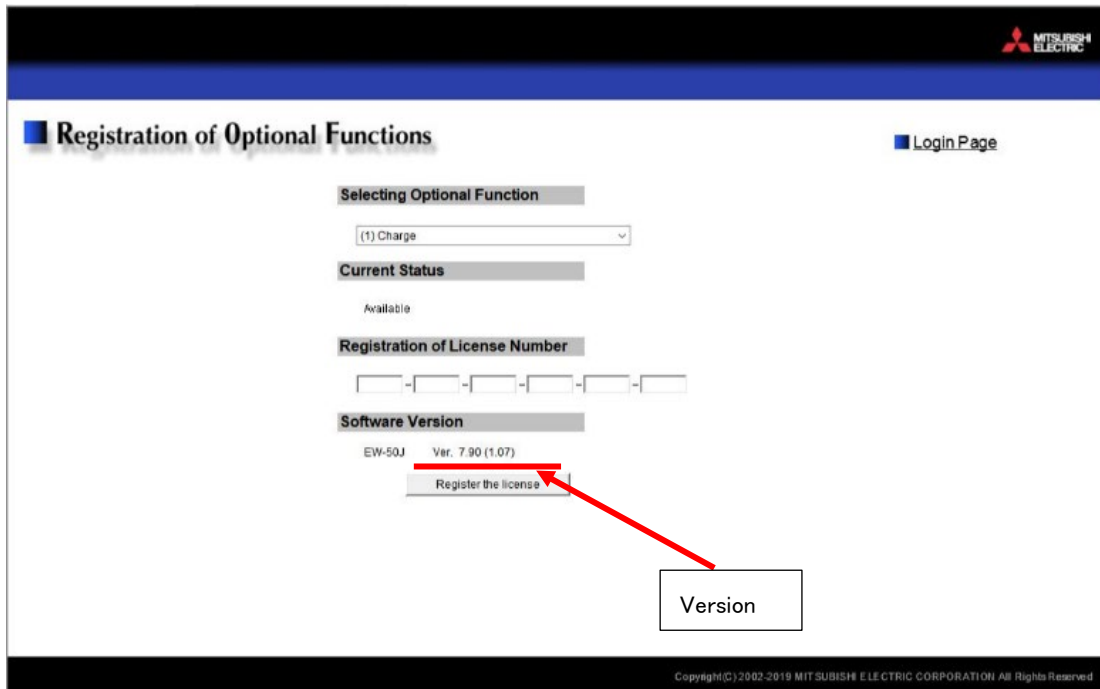
【Air Conditioning System /BM adapter】

Model	Versions
BAC-HD150	Ver.2.21 and prior

<How to check the versions>

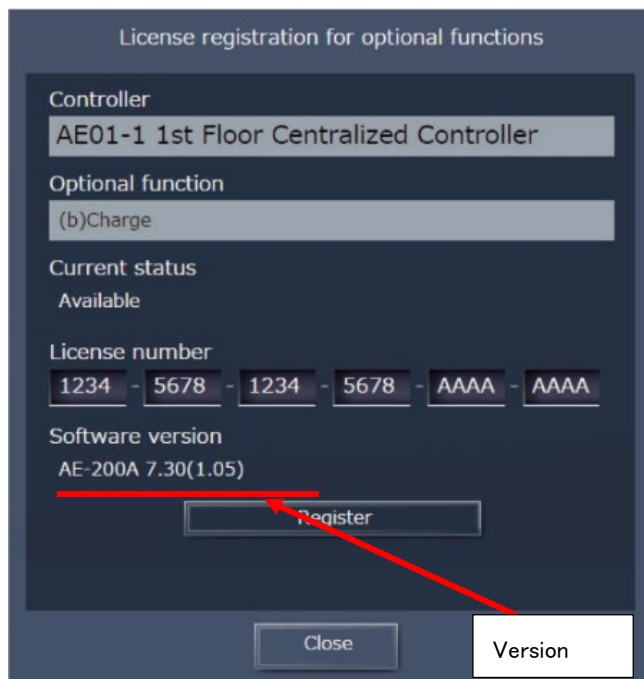
•G-50A, GB-50A, GB-24A, AG-150A-A, AG-150A-J, GB-50ADA-A, GB-50ADA-J, EB-50GU-A, EB-50GU-J, CMS-RMD-J, and PAC-YG50ECA


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

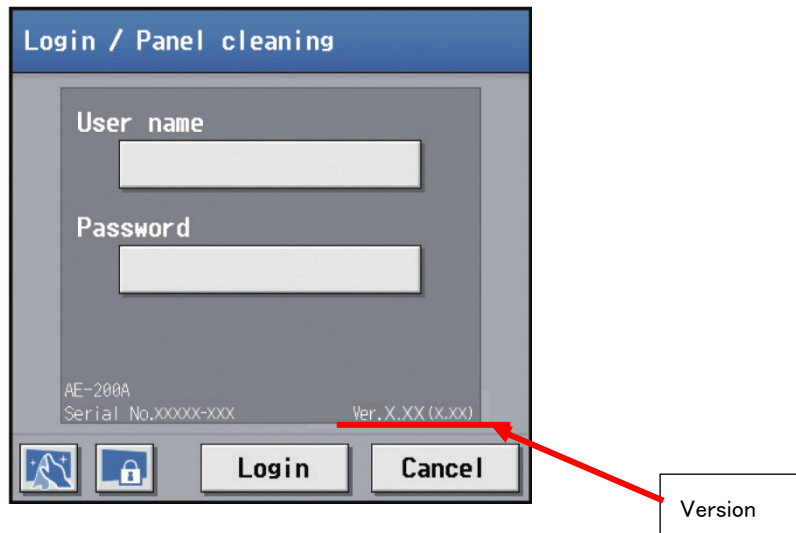


•AE-200A, AE-200E, AE-50A, AE-50E, EW-50A, EW-50E, TE-200A, TE-50A, and TW-50A

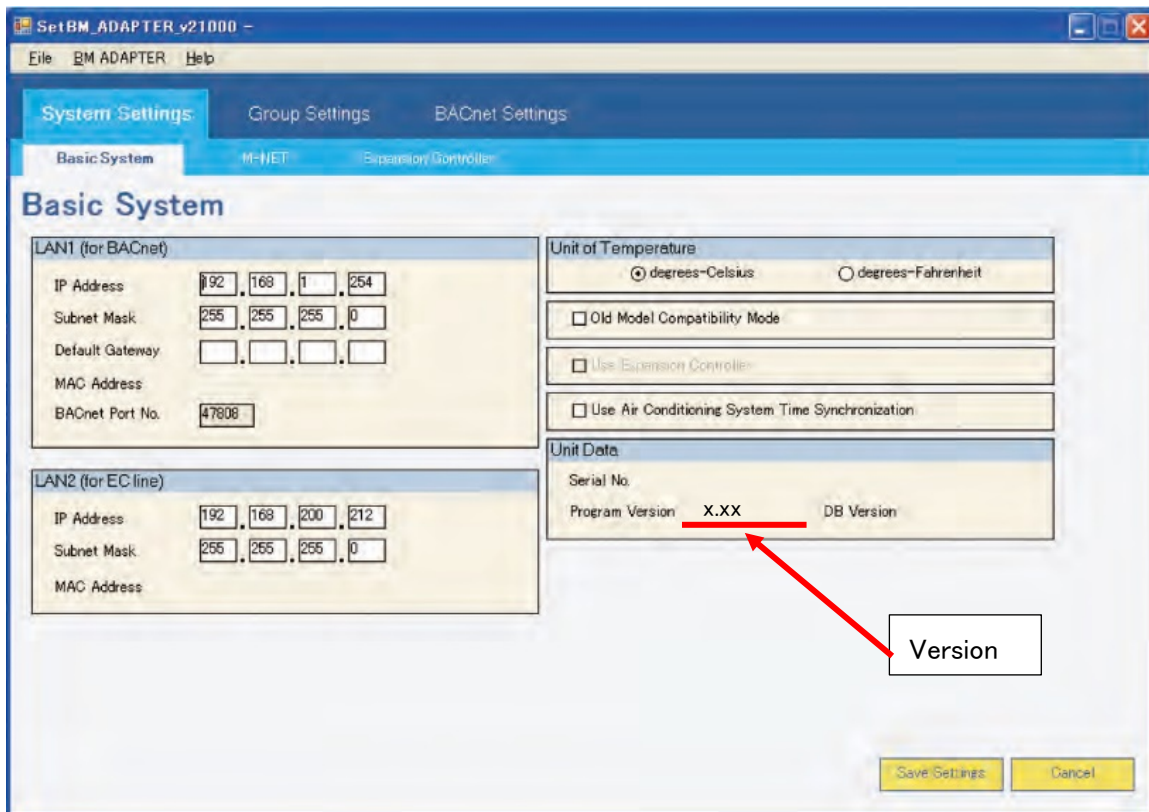
By selecting [License Registration] on Setting tab of the home screens after you log in as administrators on their WEB screen, you can check the versions.



- Another way to check versions 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.



- BAC-HD150
By clicking [Get Settings] on Basic System window of the Setting Tool, you can check the version.



■ Description

Mitsubishi Electric air conditioning systems have an information disclosure and DoS vulnerability due to improper restriction of XML external entity reference (XXE) (CWE-611).

■ Impact

A malicious attacker may disclose some of data in the air conditioning system or cause DoS condition by sending a specially crafted packet.

■ Countermeasures

The fixed 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
GB-24A	Ver.9.12 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

【Air Conditioning System /BM adapter】

Model	Versions
BAC-HD150	Ver.2.22 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 a 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.

■ Acknowledgement

Mitsubishi Electric would like to thank Howard McGreehan of Aon's Cyber Solutions who reported this vulnerability.

■ Contact information

Please contact your local Mitsubishi Electric representative.