

Information Disclosure, Information Tampering and Denial of Service Vulnerabilities in Multiple Air Conditioning Systems

Release date: June 7, 2022
Mitsubishi Electric Corporation

■ Overview

Information disclosure, information tampering and denial of service (DoS) vulnerabilities exist in encryption communications on Mitsubishi Electric air conditioning systems. A malicious attacker may disclose some of encrypted message of the air conditioning systems by sniffing encrypted communications (CVE-2022-24296, CVE-2016-2183, CVE-2013-2566, CVE-2015-2808). Besides, a man-in-the-middle attacker may tamper the message and cause a DoS condition on the air conditioning systems (CVE-2009-3555).

Mitsubishi Electric air conditioning systems are premised that they are used in intra 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-2022-24296 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score 3.1

CVE-2016-2183 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 7.5

CVE-2013-2566 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 5.9

CVE-2015-2808 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 5.9

CVE-2009-3555 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H Base Score 7.4

■ Affected products

<Models and Versions>

Explanatory note of the table below: ✓ : Affected, -: Not affected

Models	Versions	CVE-2022 -24296	CVE-2016 -2183	CVE-2013 -2566	CVE-2015 -2808	CVE-2009 -3555
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. 7.10 and prior	✓	✓	✓	✓	-
EB-50GU-J	Ver. 7.10 and prior	✓	✓	✓	✓	-
AE-200J	Ver. 7.97 and prior	✓	✓	-	-	-
AE-200A	Ver. 7.97 and prior	✓	✓	-	-	-
AE-200E	Ver. 7.97 and prior	✓	✓	-	-	-
AE-50J	Ver. 7.97 and prior	✓	✓	-	-	-
AE-50A	Ver. 7.97 and prior	✓	✓	-	-	-
AE-50E	Ver. 7.97 and prior	✓	✓	-	-	-
EW-50J	Ver. 7.97 and prior	✓	✓	-	-	-
EW-50A	Ver. 7.97 and prior	✓	✓	-	-	-
EW-50E	Ver. 7.97 and prior	✓	✓	-	-	-
TE-200A	Ver. 7.97 and prior	✓	✓	-	-	-
TE-50A	Ver. 7.97 and prior	✓	✓	-	-	-
TW-50A	Ver. 7.97 and prior	✓	✓	-	-	-

<How to check the versions>

- G-150AD, AG-150A-A, AG-150A-J, GB-50AD, GB-50ADA-A, GB-50ADA-J, EB-50GU-A and EB-50GU-J

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

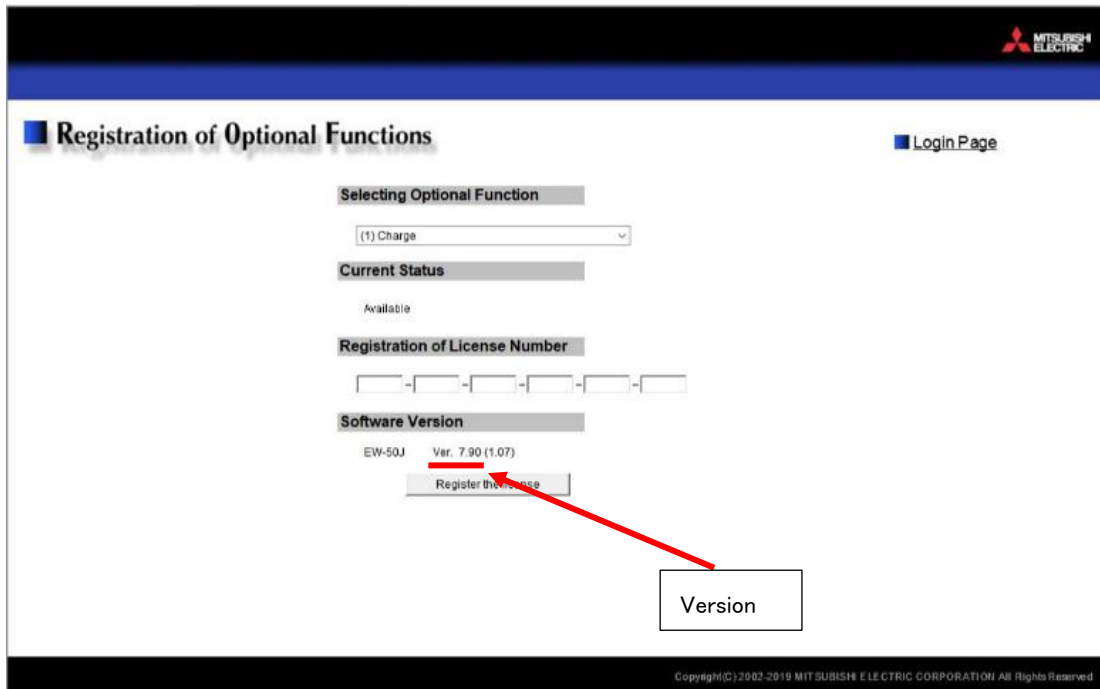


Figure 1 How to check the versions on G-150AD, AG-150A-A, AG-150A-J, GB-50AD, GB-50ADA-A, GB-50ADA-J, EB-50GU-A and EB-50GU-J

- 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 of the home screens after you log in as administrators on their WEB screen, you can check the versions (see Figure 2).

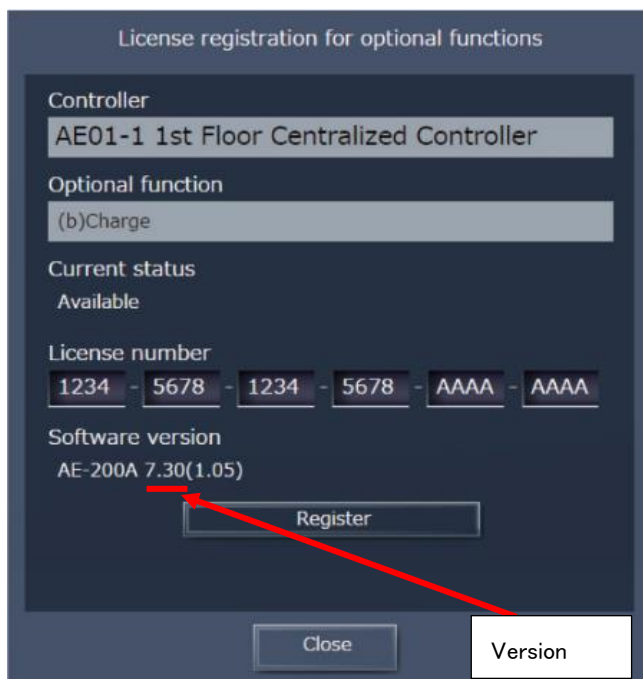



Figure 2 How to check the versions on AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, EW-50J, EW-50A, EW-50E, TE-200A, TE-50A and TW-50A

•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).

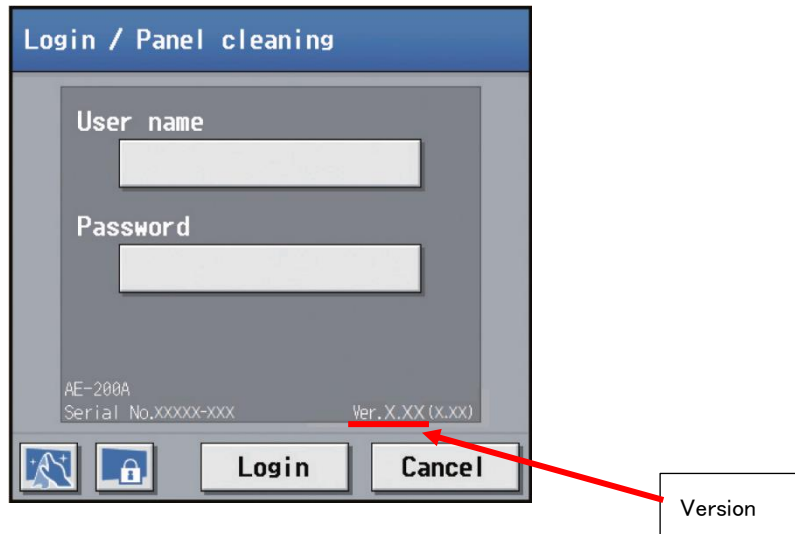


Figure 3 Another way to check the versions on G-150AD, AG-150A-A, AG-150A-J, AE-200J, AE-200A, AE-200E, AE-50J, AE-50A, AE-50E, TE-200A and TE-50A

■ Description

Information disclosure vulnerabilities (CVE-2022-24296, CVE-2016-2183, CVE-2013-2566 and CVE-2015-2808), and information tampering and denial of service (DoS) vulnerability (CVE-2009-3555) exist in encryption communications on Mitsubishi Electric air conditioning systems.

- CVE-2022-24296: Use of a Broken or Risky Cryptographic Algorithm (CWE-327)
- CVE-2016-2183: Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)
- CVE-2013-2566: Use of a Broken or Risky Cryptographic Algorithm (CWE-327)
- CVE-2015-2808: Use of a Broken or Risky Cryptographic Algorithm (CWE-327)
- CVE-2009-3555: Channel Accessible by Non-Endpoint (CWE-300)

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

In case of System Example 3, if an attacker tries to exploit the vulnerabilities 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 intra networks (Figure 4)

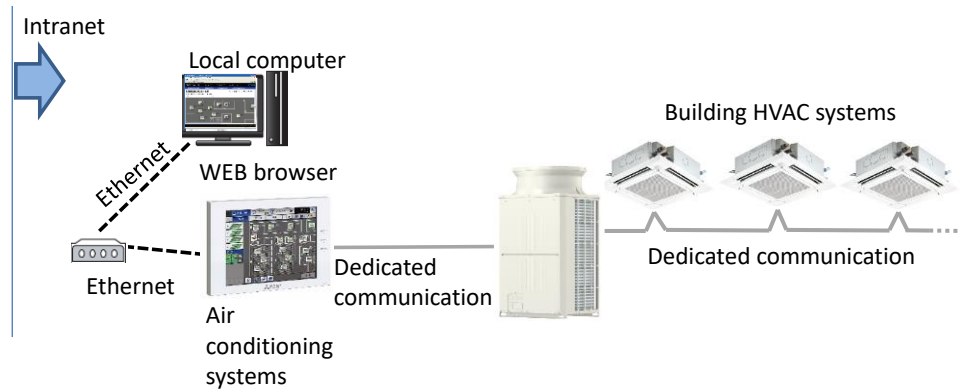


Figure 4 System Example 1

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

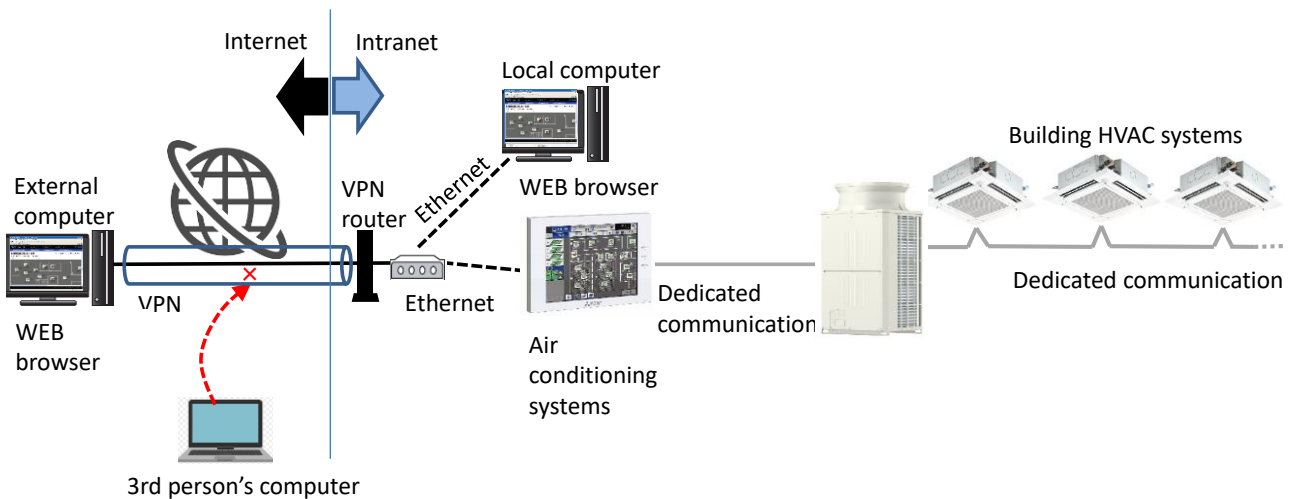


Figure 5 System Example 2

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

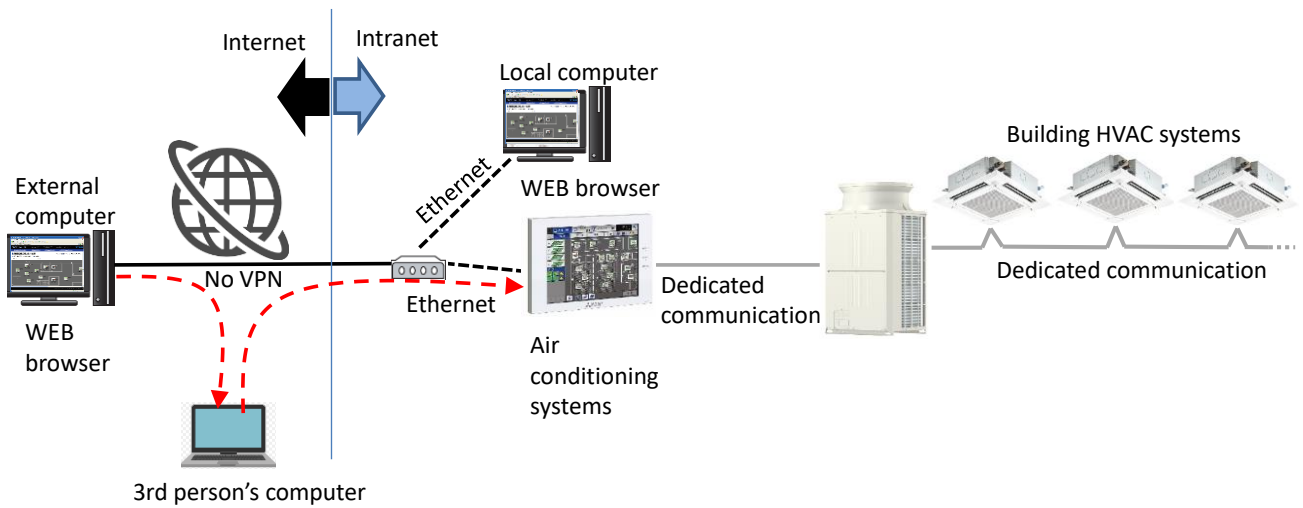


Figure 6 System Example 3

■ Impact

A malicious attacker may disclose or tamper some of data on communication between the air conditioning system and the external computers, or cause a DoS condition on the air conditioning systems.

■ Countermeasures

The fixed versions are as follows:

<Models and Versions>

Models	Versions
G-150AD	Replace the air conditioning systems to AE-200J, AE-50J or EW-50J version 7.98 or later.
AG-150A-A	Replace the air conditioning systems to AE-200A, AE-50A or EW-50A version 7.98 or later.
AG-150A-J	Replace the air conditioning systems to AE-200E, AE-50E or EW-50E version 7.98 or later.
GB-50AD	Replace the air conditioning systems to AE-200J, AE-50J or EW-50J version 7.98 or later.
GB-50ADA-A	Replace the air conditioning systems to AE-200A, AE-50A or EW-50A version 7.98 or later.
GB-50ADA-J	Replace the air conditioning systems to AE-200E, AE-50E or EW-50E version 7.98 or later.
EB-50GU-A	Ver. 7.11 or later
EB-50GU-J	Ver. 7.11 or later
AE-200J	Ver. 7.98 or later
AE-200A	Ver. 7.98 or later
AE-200E	Ver. 7.98 or later
AE-50J	Ver. 7.98 or later
AE-50A	Ver. 7.98 or later
AE-50E	Ver. 7.98 or later
EW-50J	Ver. 7.98 or later
EW-50A	Ver. 7.98 or later
EW-50E	Ver. 7.98 or later
TE-200A	Ver. 7.98 or later
TE-50A	Ver. 7.98 or later
TW-50A	Ver. 7.98 or later

<How to update>

Please contact the distributor or Mitsubishi Electric representative.

When you update the firmware, please update the OS and the browser on your computer to the latest version in addition. If the OS and the browser on your computer are old or their settings are changed, the screen below may be displayed after firmware updates and then the computer cannot connect to the air conditioning systems.

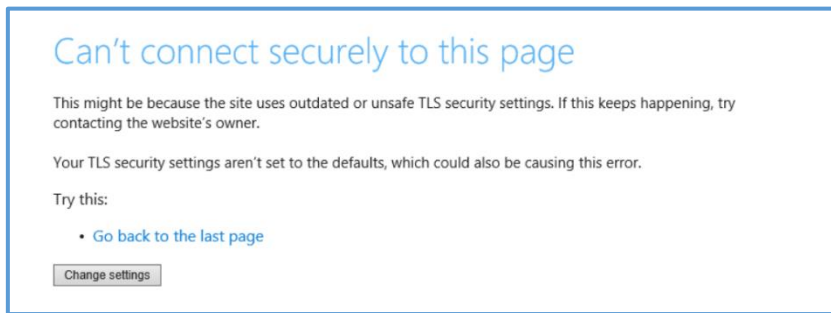


Figure 7 An example of an error on the browser

■ Mitigations

To minimize the risk of these vulnerabilities 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.

- Restrict the access to your air conditioning system from untrusted networks and hosts.
- 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.

■ Contact information

Please contact your local Mitsubishi Electric representative.