Multiple vulnerabilities in Wireless Communication Standards IEEE 802.11 (Frag Attacks)

Release date: September 2, 2021
Mitsubishi Electric Corporation

■Overview

There are multiple vulnerabilities due to design flaws in the frame fragmentation functionality and the frame aggregation functionality in Wireless Communication Standards IEEE 802.11. These vulnerabilities could allow an attacker to steal communication contents or inject unauthorized packets. The following are the product names affected by these vulnerabilities, please take workarounds.

■CVSS

[A] CVE-2020-24586: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score:3.5
[B] CVE-2020-24587: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score:2.6
[C] CVE-2020-24588: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N Base Score:3.5
[D] CVE-2020-26139: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:5.3
[E] CVE-2020-26140: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:6.5
[F] CVE-2020-26142: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:7.5
[G] CVE-2020-26143: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:6.5
[H] CVE-2020-26144: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:6.5
[I] CVE-2020-26145: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:6.5
[J] CVE-2020-26146: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:5.3
[K] CVE-2020-26147: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N Base Score:5.4

■Description

12 vulnerabilities have been found in Wireless Communication Standards IEEE 802.11. These vulnerabilities are called “FragAttacks” and could allow an attacker to steal communication contents or inject unauthorized packets. Please check the following 11 ([A] – [K]) of the 12 vulnerabilities that may affect each product in “Affected products, countermeasures, and mitigations or workarounds”.

[A] Fragment cache attack (not clearing fragments from memory when (re)connecting to a network) (CVE-2020-24586) (CWE-212)
[B] Mixed key attack (reassembling fragments encrypted under different keys) (CVE-2020-24587) (CWE-326)
[C] Aggregation attack (accepting non-SPP A-MSDU frames) (CVE-2020-24588) (CWE-306)
[D] Forwarding EAPOL frames even though the sender is not yet authenticated (should only affect APs) (CVE-2020-26139) (CWE-287)
[E] Accepting plaintext data frames in a protected network (CVE-2020-26140) (CWE-74)
[F] Processing fragmented frames as full frames (CVE-2020-26142) (CWE-74)
[G] Accepting fragmented plaintext data frames in a protected network (CVE-2020-26143) (CWE-20)
[H] Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network) (CVE-2020-26144) (CWE-20)
[I] Accepting plaintext broadcast fragments as full frames (in an encrypted network) (CVE-2020-26145) (CWE-20)
[J] Reassembling encrypted fragments with non-consecutive packet numbers (CVE-2020-26146) (CWE-20)
[K] Reassembling mixed encrypted/plaintext fragments (CVE-2020-26147) (CWE-74)

■Impact

These 11 vulnerabilities could allow an attacker to steal communication contents or inject unauthorized packets during frame aggregation or frame fragmentation.

■Affected products, countermeasures, and mitigations or workarounds

[1] [Wi-Fi Interfaces]

Model	Countermeasures and Mitigations/Workarounds
MAC-557IF-E MAC-558IF-E MAC-559IF-E PAC-WF010-E PAC-WHS01WF-E The above models of all versions. May be affected by [C] or[E]	<Countermeasures> Please carry out mitigation or workaround below. <Mitigations/Workarounds> 1.Check if the router settings are as follows. 1-1. Set encryption key of wireless LAN which can hardly be identified. If key is changed from initial setting, avoid consecutive numbers and guessable MAC address, and combine letters and numbers. 1-2. Do not use WEP encryption algorithm or Open authentication. 1-3. If you change the router settings, hide its presence on the internet in order to make it difficult for unauthorized access. (e.g. Set to not respond to PING request) 1-4. Set password for the router's Management portal, which is difficult to be identified. 2.Check the following when using a computer or tablet, etc. at home. 2-1. Update Antivirus software to the latest version. 2-2. Do not open or access suspicious attachment file or linked URL.

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries>

https://www.mitsubishielectric.com/en/contact/room-air-conditioners.page

[2] [Wi-Fi Interfaces and Air Conditioning]

Model	Countermeasures and Mitigations/Workarounds
Wi-Fi Interfaces: MAC-567IF-E MAC-568IF-E S-MAC-905IF S-MAC-906IF Air Conditioning: MSZ-FT20/25VFK MSZ-FX20/25VFK MSZ-GZT09/12/18VAK MSZ-GZT09/12/18VAK-1 MSZ-ZT09/12/18VAK MSZ-ZT09/12/18VAK-1 MSZ-AP25/35/42/50VGK-E6 MSZ-AP60/71VGK-E1 MSZ-AP60/71VGK-ER1 MSZ-AP60/71VGK-ET1 MSZ-LN18/25/35/50/60VGW(V)(R)(B)-E1 MSZ-LN18/25/35/50/60VG2W(V)(R)(B)-E1 MSZ-LN25/35/50/60VGW(V)(R)(B)-ER1 MSZ-LN25/35/50/60VG2W(V)(R)(B)-ER1 MSZ-LN18VG2W-ER1 MSZ-LN25/35/50/60VG2W(V)(R)(B)-ET1 MSZ-LN25/35/50VG2W(V)(R)(B)-EN1 MSZ-AP22/25/35/42/50/60/71/80VGKD-A1 MSZ-AP22/25/35/42/50/60/71/80VGKD-A2 MSZ-LN25/35/50/60VGV(R)(B)-A1 MSZ-LN25/35/50/60VG2V(R)(B)-A1 The above models of all versions. May be affected by [B],[C],[F],[H],[I],[J].	<Countermeasures> Please carry out mitigation or workaround below. <Mitigations/Workarounds> 1.Check if the router settings are as follows. 1-1. Set encryption key of wireless LAN which can hardly be identified. If key is changed from initial setting, avoid consecutive numbers and guessable MAC address, and combine letters and numbers. 1-2. Do not use WEP encryption algorithm or Open authentication. 1-3. If you change the router settings, hide its presence on the internet in order to make it difficult for unauthorized access. (e.g. Set to not respond to PING request) 1-4. Set password for the router's Management portal, which is difficult to be identified. 2.Check the following when using a computer or tablet, etc. at home. 2-1. Update Antivirus software to the latest version. 2-2. Do not open or access suspicious attachment file or linked URL.

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries>

https://www.mitsubishielectric.com/en/contact/room-air-conditioners.page

[3] [Wi-Fi Interfaces and Air Conditioning]

Model	Countermeasures and Mitigations/Workarounds
Wi-Fi Interface: S-MAC-002IF Air Conditioning: MFZ-GXT50/60/73VFK MFZ-XT50/60/73VFK MSZ-GZY09/12/18VFK MSZ-KY09/12/18VFK MSZ-WX18/20/25VFK MSZ-ZY09/12/18VFK MSZ-AP15/20/25/35/42/50VGK-E1 MSZ-AP15/20/25/35/42/50VGK-ER1 MSZ-AP15/20/25/35/42/50VGK-ET1 MSZ-AP25/35/42/50VGK-EN1 MSZ-AP15/20/25/35/42/50/60/71VGK-E2 MSZ-AP15/20/25/35/42/50/60/71VGK-ER2 MSZ-AP15/20/25/35/42/50/60/71VGK-ET2 MSZ-AP25/35/42/50VGK-EN2 MSZ-AP25/35/42/50/60/71VGK-E3 MSZ-AP25/35/42/50/60/71VGK-ER3 MSZ-AP25/35/42/50/60/71VGK-ET3 MSZ-AP25/35/42/50VGK-EN3 MSZ-AP25/35/42/50VGK-E7 MSZ-AP25/35/42/50VGK-E8 MSZ-BT20/25/35/50VGK-E1 MSZ-BT20/25/35/50VGK-E2 MSZ-BT20/25/35/50VGK-ET1 MSZ-EF18/22/25/35/42/50VGKW(S)(B)-E1 MSZ-EF22/25/35/42/50VGKW(S)(B)-ER1 MSZ-EF25VGKB-ET1 MSZ-FT25/35/50VGK-E1 MSZ-FT25/35/50VGK-ET1 MSZ-FT25/35/50VGK-SC1 MSZ-LN18/25/35/50/60VG2W(B)(R)(V)-E2 MSZ-LN25/35/50/60VG2W(B)(R)(V)-ER2 MSZ-LN25/35/50/60VG2W(B)(R)(V)-ET2 MSZ-LN25/35/50VG2W(B)(R)(V)-EN2 MSZ-RW25/35/50VG-E1 MSZ-RW25/35/50VG-ER1 MSZ-RW25/35/50VG-ET1 MSZ-RW25/35/50VG-SC1 MSZ-EF22/25/35/42/50VGKW(S)(B)-A1 MSZ-LN25/35/50/60VG2V(R)(B)-A2 The above models of version 3300 or less. “Version” is printed on Wi-Fi interface. May be affected by [A],[B],[C],[D],[E],[G], [H],[I],[J],[K].	<Countermeasures> Please carry out mitigation or workaround below. <Mitigations/Workarounds> 1.Check if the router settings are as follows. 1-1. Set encryption key of wireless LAN which can hardly be identified. If key is changed from initial setting, avoid consecutive numbers and guessable MAC address, and combine letters and numbers. 1-2. Do not use WEP encryption algorithm or Open authentication. 1-3. If you change the router settings, hide its presence on the internet in order to make it difficult for unauthorized access. (e.g. Set to not respond to PING request) 1-4. Set password for the router’s Management portal, which is difficult to be identified. 2.Check the following when using a computer or tablet, etc. at home. 2-1. Update Antivirus software to the latest version. 2-2. Do not open or access suspicious attachment file or linked URL.

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries>

https://www.mitsubishielectric.com/en/contact/room-air-conditioners.page