Information Disclosure Vulnerability in multiple consumer electronics products

Release date: September 29, 2022
Mitsubishi Electric Corporation

■Overview

Information disclosure vulnerability due to the use of Basic Authentication for HTTP connections exists in multiple consumer electronics products manufactured by Mitsubishi Electric Corporation. Basic Authentication for HTTP connections allows a third party to obtain credential information (username and password) by sniffing, leading to unauthorized access. This vulnerability allows a malicious attacker to disclose information in the product or cause a denial of service (DoS) condition as a result (CVE-2022-33321). The names of products affected by this vulnerability are listed below, please take countermeasures, mitigations and workarounds.

■CVSS Score

CVE-2022-33321　CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N　Base Score:5.9

■Description

Multiple consumer electronics products manufactured by Mitsubishi Electric use Basic Authentication for HTTP connections. In Basic Authentication, the credential information (username and password) is encoded in Base64 and sent to the Web server. The credential information (username and password) is not encrypted. Therefore, if Basic Authentication is used for HTTP connections where the communication data flows in plain text, a third party can obtain the credential information (username and password) by sniffing. (CWE-319)

■Impact

Disclosure of credential information (username and password) to a third party leads to unauthorized access. This vulnerability allows a malicious attacker to disclose information in the product or cause a denial of service (DoS) condition as a result.

■Affected products, countermeasures, and mitigations or workarounds

[1] [Wi-Fi Interface and Air Conditioning]

model number	Countermeasures and Mitigation/Workarounds
Wi-Fi Interface: MAC-557IF-E MAC-557IF-E1 PAC-WF010-E MAC-566IFB-E MAC-576IF-E1 MAC-567IFB-E MAC-567IFB2-E MAC-558IF-E MAC-558IF-E1 MAC-559IF-E MAC-559IF-E1 MAC-568IF-E MAC-568IFB-E MAC-568IFB2-E MAC-568IFB3-E PAC-WHS01WF-E S-MAC-702IF-F S-MAC-702IF-Z S-MAC-702IF-B S-MAC-905IF S-MAC-906IF Air Conditioning: MSZ-AP60/71VGK-E1 MSZ-AP60/71VGK-ER1 MSZ-AP60/71VGK-ET1 MSZ-AP25/35/42/50VGK-E6 MSZ-LN18/25/35/50/60VGW-E1 MSZ-LN18/25/35/50/60VGV-E1 MSZ-LN18/25/35/50/60VGB-E1 MSZ-LN18/25/35/50/60VGR-E1 MSZ-LN25/35/50/60VGW-ER1 MSZ-LN25/35/50/60VGV-ER1 MSZ-LN25/35/50/60VGB-ER1 MSZ-LN25/35/50/60VGR-ER1 MSZ-LN18/25/35/50/60VG2W-E1 MSZ-LN18/25/35/50/60VG2V-E1 MSZ-LN18/25/35/50/60VG2B-E1 MSZ-LN18/25/35/50/60VG2R-E1 MSZ-LN18/25/35/50/60VG2W-ER1 MSZ-LN25/35/50/60VG2V-ER1 MSZ-LN25/35/50/60VG2B-ER1 MSZ-LN25/35/50/60VG2R-ER1 MSZ-LN18/25/35/50/60VG2W-ET1 MSZ-LN18/25/35/50/60VG2V-ET1 MSZ-LN18/25/35/50/60VG2B-ET1 MSZ-LN18/25/35/50/60VG2R-ET1 MSZ-LN18/25/35/50VG2W-EN1 MSZ-LN18/25/35/50VG2V-EN1 MSZ-LN18/25/35/50VG2B-EN1 MSZ-LN18/25/35/50VG2R-EN1 MSZ-LN25/35/50/60VGV-A1 MSZ-LN25/35/50/60VGB-A1 MSZ-LN25/35/50/60VGR-A1 MSZ-LN25/35/50/60VG2V-A1 MSZ-LN25/35/50/60VG2B-A1 MSZ-LN25/35/50/60VG2R-A1 MSZ-FT20/25VFK MSZ-FX20/25VFK MSZ-GZT09/12/18VAK MSZ-ZT09/12/18VAK	<Impact> This vulnerability allows a malicious attacker to disclose information in the product or cause a denial of service (DoS) condition as a result. <Countermeasures> Please carry out the mitigations below. <Mitigations/Workarounds> 1.Check if the wireless LAN 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 wireless LAN 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 wireless LAN router's Management portal, which is difficult to be identified. 1-5. Install the wireless LAN router in a location where it cannot be touched by outsiders. Do not open the network to unspecified third parties, such as by offering it as free Wi-Fi. 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.

All versions of the above models are affected. Wi-Fi Interface: MAC-587IF-E MAC-587IF2-E MAC-507IF-E MAC-588IF-E S-MAC-002IF Air Conditioning: MSXY-FP05/07/10/13/18/20/24VGK-SG1 MSY-GP10/13/15/18/20/24VFK-SG1 MSZ-AP25/35/42/50VGK-E1 MSZ-AP15/20/25/35/42/50/60/71VGK-E2 MSZ-AP25/35/42/50/60/71VGK-E3 MSZ-AP25/35/42/50VGK-E7 MSZ-AP25/35/42/50VGK-E8 MSZ-AP25/35/42/50VGK-EN1 MSZ-AP25/35/42/50VGK-EN2 MSZ-AP25/35/42/50VGK-EN3 MSZ-AP25/35/42/50VGK-ER1 MSZ-AP15/20/25/35/42/50/60/71VGK-ER2 MSZ-AP25/35/42/50/60/71VGK-ER3 MSZ-AP25/35/42/50VGK-ET1 MSZ-AP15/20/25/35/42/50/60/71VGK-ET2 MSZ-AP25/35/42/50/60/71VGK-ET3 MSZ-AY25/35/42/50VGK-E1 MSZ-AY25/35/42/50VGK-E6 MSZ-AY25/35/42/50VGK-ER1 MSZ-AY25/35/42/50VGK-ET1 MSZ-AY25/35/42/50VGK-SC1 MSZ-AY25/35/42/50VGKP-E6 MSZ-AY25/35/42/50VGKP-ER1 MSZ-AY25/35/42/50VGKP-ET1 MSZ-AY25/35/42/50VGKP-SC1 MSZ-BT20/25/35/50VGK-E1 MSZ-BT20/25/35/50VGK-E2 MSZ-BT20/25/35/50VGK-E3 MSZ-BT20/25/35/50VGK-ER1 MSZ-BT20/25/35/50VGK-ER2 MSZ-BT20/25/35/50VGK-ET1 MSZ-BT20/25/35/50VGK-ET2 MSZ-BT20/25/35/50VGK-ET3 MSZ-EF18/22/25/35/42/50VGKW-E1 MSZ-EF18/22/25/35/42/50VGKB-E1 MSZ-EF18/22/25/35/42/50VGKS-E1 MSZ-EF18/22/25/35/42/50VGKW-E2 MSZ-EF18/22/25/35/42/50VGKB-E2 MSZ-EF18/22/25/35/42/50VGKS-E2 MSZ-EF22/25/35/42/50VGKW-ER1 MSZ-EF22/25/35/42/50VGKB-ER1 MSZ-EF22/25/35/42/50VGKS-ER1 MSZ-EF22/25/35/42/50VGKW-ER2 MSZ-EF22/25/35/42/50VGKB-ER2 MSZ-EF22/25/35/42/50VGKS-ER2 MSZ-EF22/25/35/42/50VGKW-ET1 MSZ-EF22/25/35/42/50VGKB-ET1 MSZ-EF22/25/35/42/50VGKS-ET1 MSZ-EF22/25/35/42/50VGKW-ET2 MSZ-EF22/25/35/42/50VGKB-ET2 MSZ-EF22/25/35/42/50VGKS-ET2 MSZ-FT25/35/50VGK-E1 MSZ-FT25/35/50VGK-E2 MSZ-FT25/35/50VGK-ET1 MSZ-FT25/35/50VGK-SC1 MSZ-FT25/35/50VGK-SC2	

MSZ-HR25/35/42/50/60/71VFK-E1 MSZ-HR25/35/42/50VFK-E6 MSZ-HR25/35/42/50/60/71VFK-ER1 MSZ-HR25/35/42/50/60/71VFK-ET1 MSZ-LN18/25/35/50/60VG2W-E2 MSZ-LN18/25/35/50/60VG2W-E3 MSZ-LN25/35/50VG2W-EN2 MSZ-LN18/25/35/50/60VG2W-ER2 MSZ-LN25/35/50/60VG2W-ER3 MSZ-LN18/25/35/50/60VG2W-ET2 MSZ-LN25/35/50/60VG2W-ET3 MSZ-LN18/25/35/50/60VG2V-E2 MSZ-LN18/25/35/50/60VG2V-E3 MSZ-LN25/35/50VG2V-EN2 MSZ-LN25/35/50/60VG2V-ER2 MSZ-LN25/35/50/60VG2V-ER3 MSZ-LN25/35/50/60VG2V-ET2 MSZ-LN25/35/50/60VG2V-ET3 MSZ-LN18/25/35/50/60VG2B-E2 MSZ-LN18/25/35/50/60VG2B-E3 MSZ-LN25/35/50VG2B-EN2 MSZ-LN25/35/50/60VG2B-ER2 MSZ-LN25/35/50/60VG2B-ER3 MSZ-LN25/35/50/60VG2B-ET2 MSZ-LN25/35/50/60VG2B-ET3 MSZ-LN18/25/35/50/60VG2R-E2 MSZ-LN18/25/35/50/60VG2R-E3 MSZ-LN25/35/50VG2R-EN2 MSZ-LN25/35/50/60VG2R-ER2 MSZ-LN25/35/50/60VG2R-ER3 MSZ-LN25/35/50/60VG2R-ET2 MSZ-LN25/35/50/60VG2R-ET3 MSZ-LN18/25/35/50VG2W-SC1 MSZ-LN25/35/50VG2V-SC1 MSZ-LN25/35/50VG2B-SC1 MSZ-LN25/35/50VG2R-SC1 MSZ-RW25/35/50VG-E1 MSZ-RW25/35/50VG-ER1 MSZ-RW25/35/50VG-ET1 MSZ-RW25/35/50VG-SC1 MSZ-AP22/25/35/42/50/61/70/80VGKD-A1 MSZ-AP22/25/35/42/50/60/71/80VGKD-A2 MSZ-EF22/25/35/42/50VGKW-A1 MSZ-EF22/25/35/42/50VGKB-A1 MSZ-EF22/25/35/42/50VGKS-A1 MSZ-LN25/35/50/60VG2V-A2 MSZ-LN25/35/50/60VG2B-A2 MSZ-LN25/35/50/60VG2R-A2 MFZ-GXT50/60/73VFK MFZ-XT50/60VFK MSZ-EZA09/12VAK MSZ-EXA09/12VAK MSZ-GZY09/12/18VFK MSZ-KY09/12/18VFK MSZ-WX18/20/25VFK MSZ-ZY09/12/18VFK Versions 35.00 and prior of the above models are affected.	

*Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries> https://www.mitsubishielectric.com/en/contact/room-air-conditioners.html

[2] [Air Purifier]

model number	Countermeasures and Mitigation/Workarounds
MA-EW85S-E MA-EW85S-UK Versions 80.00 and prior of the above models are affected.	<Impact> This vulnerability allows a malicious attacker to disclose information in the product or cause a denial of service (DoS) condition as a result. <Countermeasures> Please carry out the mitigations below. <Mitigations/Workarounds> 1.Check if the wireless LAN 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 wireless LAN 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 wireless LAN router's Management portal, which is difficult to be identified. 1-5. Install the wireless LAN router in a location where it cannot be touched by outsiders. Do not open the network to unspecified third parties, such as by offering it as free Wi-Fi. 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/products-solutions/home/index.html