TLP:WHITE

# ICS Advisory (ICSA-21-252-03)

More ICS-CERT Advisories

## Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU

Original release date: September 09, 2021

## Legal Notice



## 1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Mitsubishi Electric Europe B.V.
- **Equipment:** smartRTU and INEA ME-RTU
- **Vulnerabilities:** OS Command Injection, Improper Access Control, Cross-site Scripting, Use of Hard-coded Credentials, Unprotected Storage of Credentials, Incorrect Default Permissions

## 2. REPOSTED INFORMATION

This advisory is a follow-up to a CISA product update titled ICS-ALERT-19-225-01 Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A) published September 10, 2019, on the ICS webpage on us-cert.cisa.gov.

## 3. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to gain remote code execution, obtain credentials, and use credentials found to log into other affected devices.

# 4. TECHNICAL DETAILS

## 4.1 AFFECTED PRODUCTS

TLP:WHITE

The following products are affected:

- smartRTU and INEA ME-RTU: All firmware versions prior to Version 3.3

## 4.2 VULNERABILITY OVERVIEW

### 4.2.1 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS COMMAND INJECTION') CWE-78

The affected product allows an attacker to execute arbitrary commands due to the passing of unsafe user supplied data to the system shell.

CVE-2019-14931 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

### 4.2.2 IMPROPER ACCESS CONTROL CWE-284

It is possible to download the affected product's configuration file, which contains sensitive data, through the URL.

CVE-2019-14927 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

### 4.2.3 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79

The affected product's web configuration software allows an authenticated user to inject malicious data into the application that can then be executed in a victim's browser, allowing stored cross-site scripting.

CVE-2019-14928 has been assigned to this vulnerability. A CVSS v3 base score of 5.4 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).

### 4.2.4 USE OF HARD-CODED CREDENTIALS CWE-798

Hard-coded SSH keys have been identified in the affected product's firmware. As the secure keys cannot be regenerated by a user and are not regenerated on firmware updates, all deployed affected products utilize the same SSH keys.

CVE-2019-14926 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

### 4.2.5 USE OF HARD-CODED CREDENTIALS CWE-798

The affected products contain undocumented user accounts with hard-coded password credentials. An attacker could exploit this vulnerability by using the accounts to login to affected RTU's.

CVE-2019-14930 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

### 4.2.6 UNPROTECTED STORAGE OF CREDENTIALS CWE-256

The affected products store password credentials in plain text in a configuration file. An unauthenticated user can obtain the exposed password credentials to gain access to the specific services.

CVE-2019-14929 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

### 4.2.7 INCORRECT DEFAULT PERMISSIONS CWE-276

The affected products store and reads configuration settings from a file that has insecure world-readable permissions assigned. This could allow all users on the system to read the configuration file containing usernames and plain text password combinations, as well as other sensitive configuration information of the RTU.

CVE-2019-14925 has been assigned to this vulnerability. A CVSS v3 base score of 6.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).

## 4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Japan

## 4.4 RESEARCHER

Mark Cross (@xerubus) reported these vulnerabilities to CISA.

# 5. MITIGATIONS

Mitsubishi Electric Europe B.V. recommends users update to firmware Version 3.3 or later.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

Known public exploits specifically target these vulnerabilities.

## Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

---