Authentication Bypass Vulnerability and OS Command Injection Vulnerability in smartRTU module

Release date: April 4, 2025
Mitsubishi Electric Europe B.V.

Overview

Authentication bypass vulnerability and OS command injection vulnerability exist in the Mitsubishi Electric B.V. smartRTU module. A remote unauthenticated attacker may be able to bypass authentication and execute arbitrary OS commands by utilizing a specific API route to disclose, tamper with, destroy or delete information in the product, or cause a denial-of service (DoS) condition on the product (CVE-2025-3128, CVE-2025-3232).

CVSS[1]

CVE-2025-3232	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Base Score:	7.5
CVE-2025-3128	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:	9.8

Affected products

<Affected products and versions>
Mitsubishi Electric Europe B.V. smartRTU version 3.37 and prior

<How to check your product version>
Open the module's Web Interface and navigate to the “General” tab, “RTU Operating mode” (Figure 1).

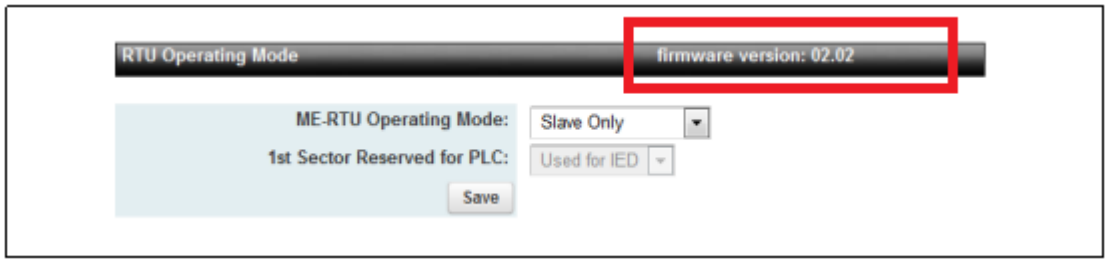

Figure 1 ME-RTU Firmware Version screen

Description

Authentication bypass vulnerability due to Missing Authentication for Critical Function (CWE-306[2]) and OS command injection vulnerability due to Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78[3]) exist in the Mitsubishi Electric B.V. smartRTU module.

Impact

A remote unauthenticated attacker may be able to bypass authentication and execute arbitrary OS commands by utilizing a specific API route to disclose, tamper with, destroy or delete information in the product, or cause a denial-of service (DoS) condition on the product.

Countermeasures

There are no plans to release a fixed version, so we kindly ask you to address this issue through mitigations and workarounds.

Mitigations / Workarounds

Mitsubishi Electric Europe B.V. recommends that customers take note of the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use WAF (Web Application Firewall) to prevent to filter, monitor and block any malicious HTTP/HTTPS traffic
- Allow web client access from trusted networks only.

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/306.html

[3] https://cwe.mitre.org/data/definitions/78.html

Acknowledgement

Mitsubishi Electric Europe B.V. would like to thank Noam Moshe of Claroty Team82 who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric Europe B.V. Factory Automation representative.
https://de.mitsubishielectric.com/fa/de_en/contact