March 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Schneider Electric published security advisories to highlight vulnerabilities in the following products:

- Easergy T200 – multiple versions and platforms
- EcoStruxure Power Design Ecodial – multiple versions and platforms

Technical Details

The Easergy T200 RTU Product Line (T200I, T200E, T200P) is a modular platform for medium voltage and low voltage public distribution network management. Note, this product has been obsoleted since December 31st, 2021, and is no longer available for purchase. Failure to apply the remediations provided below may allow a brute force attack, which could result in unauthorized data access, and/or compromise of the device.

Affected Products and Models

Product	Version
Easergy T200 (Modbus) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04MOD-07000104** and prior
Easergy T200 (IEC104) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04IEC-07000104** and prior
Easergy T200 (DNP3) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04DNP-07000104** and prior

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-2051 CVE-2024-2050 CVE-2024-2052
- Schneider Electric Security Notification - SEVD-2024-072-01 (PDF)
- Schneider Electric Security Notification - SEVD-2024-072-02 (PDF)
- Schneider Electric Security Notifications