February 13, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin 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:

- EcoStruxure Control Expert – versions prior to v16.0
- EcoStruxure IT Gateway – versions 1.20.x and prior
- EcoStruxure Process Expert – versions prior to v2023
- Modicon M340 CPU – versions prior to sv3.60
- Modicon M580 CPU – versions prior to sv4.20
- Modicon M580 CPU Safety – all versions
- Harmony Control Relay RMNF22TB30 – all versions
- Harmony Timer Relay RENF22R2MMW – all versions

Technical Details

CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause a denial of service and loss of confidentiality, integrity of controllers when conducting a Man in the Middle attack.
These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-6408 CVE-2023-6409 CVE-2023-27975
- Schneider Electric Security Notification - SEVD-2024-044-01 (PDF)
- Schneider Electric Security Notification - SEVD-2024-044-02 (PDF)
- Schneider Electric Security Notification - SEVD-2024-044-03 (PDF)
- Schneider Electric Security Notifications