December 8, 2023

Overall rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Schweitzer Engineering Laboratories SEL-411L vulnerability. The vulnerability affects versions R118: V0 - V4, R119: V0 - V5, R120: V0 - V6, R121: V0 - V3, R122: V0 - V3, R123: V0 - V3, R124: V0 - V3, R125: V0 - V3, R126: V0 - V4, R127: V0 - V2, R128: V0 - V1, and R129: V0 - V1. Successful exploitation of this vulnerability could expose authorized users to clickjacking attacks.

Technical Details

An Improper Restriction of Rendered UI Layers or Frames in the Schweitzer Engineering Laboratories SEL-411L could allow an unauthenticated attacker to perform clickjacking-based attacks against an authenticated and authorized user.

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

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk.

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-2023-2265
- ICSA-23-341-02 Schweitzer Engineering Laboratories SEL-411L
- VRM Vulnerability Reports