January 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Rapid Software vulnerabilities impacting the energy and transportation sectors. The vulnerability affects Rapid SCADA versions 5.8.4 and prior.

Technical Details

Successful exploitation of these vulnerabilities could result in an attacker reading sensitive files from the Rapid Scada server, writing files to the Rapid Scada directory (thus achieving code execution), gaining access to sensitive systems via legitimate-seeming phishing attacks, connecting to the server and preforming attacks using the high privileges of a service, obtaining administrator passwords, learning sensitive information about the internal code of the application, or achieving remote code execution.

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 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-2024-21852, CVE-2024-22096, CVE-2024-22016, CVE-2024-21794, CVE-2024-21764, CVE-2024-21869, CVE-2024-21866
- ICSA-24-011-03 Rapid Software LLC Rapid SCADA
- VRM Vulnerability Reports