

Overall rating: Critical



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 advisories to address vulnerabilities in the following products:

- Easy UPS Online Monitoring Software – version 2.6-GA-01-23116 and prior
- Trio Q-Series Ethernet Data Radio – all versions
- Trio E-Series Ethernet Data Radio – all versions
- Trio J-Series Ethernet Data Radio – all versions
- Plant iT/Brewmaxx – version v9.60 and later

Technical Details

CVSS v3.1 Base Score 10.0 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H It was discovered, that Redis, a persistent key-value database, due to a packaging issue, is prone to a Lua sandbox escape, which could result in remote code execution. Note: The original CVE description from Redis has been modified in the context of Plant iT.

These vulnerabilities are rated as an overall **Critical** 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-2023-6407, CVE-2023-5629, CVE-2022-0543
- [Schneider Electric Security Notification - SEVD-2023-346-03 \(PDF\)](#)
- [Schneider Electric Security Notification - SEVD-2023-346-01 \(PDF\)](#)
- [Schneider Electric Security Notification - SEVD-2023-346-02 \(PDF\)](#)
- [Schneider Electric Security Notifications](#)
-