

## Overall Rating - High



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 a security advisory to highlight a vulnerability in the following product:

- Easergy Studio – versions prior to 9.3.3

### Technical Details

CVE ID: CVE-2024-2747 CVSS v3.1 Base Score 7.8 | High |  
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-428: Unquoted search path or element vulnerability exists in Easergy Studio, which could cause privilege escalation when a valid user replaces a trusted file name on the system and reboots the machine.  
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-2024-2747
- [Schneider Electric Security Notification - SEVD-2024-100-01 \(PDF\)](#)
- [Schneider Electric Security Notifications](#)