



CVE-2022-24318

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-24318 |
| State | PUBLIC |
| Assigner | cybersecurity@schneider-electric.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-02-09 23:15:00 UTC |
| Updated | 2022-02-17 04:08:00 UTC |
| Description | A CWE-326: Inadequate Encryption Strength vulnerability exists that could cause non-encrypted communication with the se |

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------------------|-----------------------------------|---------|--------|---------|----------|
| Application | Schneider-electric | Clearscada | All | All | All | All |
| Application | Schneider-electric | Ecostruxure Geo Scada Expert 2019 | All | All | All | All |
| Application | Schneider-electric | Ecostruxure Geo Scada Expert 2020 | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|---------------------|
| download.schneider-electric.com/files | MISC | download.schneider-electric.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590722](#) Schneider Electric EcoStruxure Geo SCADA Expert Multiple Vulnerabilities (SEVD-2022-039-05)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report