



CVE-2023-5391

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

Summary

CVE	CVE-2023-5391
State	PUBLIC
Assigner	cybersecurity@schneider-electric.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-04 19:15:00 UTC
Updated	2024-02-01 00:49:00 UTC
Description	A CWE-502: Deserialization of untrusted data vulnerability exists that could allow an attacker to execute arbitrary code on the

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Ecostruxure Power Monitoring Expert	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Operation With Advanced Reports	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Scada Operation With Advanced Reports	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.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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