CVE-2025-13845

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-13845
State	PUBLISHED
Assigner	schneider
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-15 19:16:02 UTC
Updated	2026-04-27 17:26:56 UTC
Description	CWE-416: Use After Free vulnerability that could cause remote code execution when the end user imports the malicious pr

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from cybersecurity@se.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000360000 probability, percentile 0.106140000 (date 2026-04-27)

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
4.0	cybersecurity@se.com	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All

Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All
Application	Schneider-electric	Ecostruxure Power Build - Rapsody	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected FR v2.8.1.0300 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected ESP v2.8.5.0200 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected PT v2.8.7.0100 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected BEL (FR) v2.8.8.0100 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected BEL (EN) v2.8.3.0100 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected INT (EN) v2.8.4.0300 and prior	Not specified
CNA	Schneider Electric	EcoStruxure Power Build Rapsody	affected NL v2.8.2.0000 and prior	Not specified

References

Reference	Source	Link	Tags
download.schneider-electric.com/files	cybersecurity@se.com	download.schneider-electric.com	Vendor Advisory
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.