Sparx Enterprise Architect Client reveals plaintext OAuth2 client secret

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

Summary

CVE	CVE-2025-15622
State	PUBLISHED
Assigner	NCSC-FI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 09:16:03 UTC
Updated	2026-04-17 15:13:15 UTC
Description	Insufficiently Protected Credentials vulnerability in Sparx Systems Pty Ltd. Sparx Enterprise Architect. Client reveals plainte

Risk And Classification

Primary CVSS: v4.0 6.2 MEDIUM from db4dfee8-a97e-4877-bfae-eba6d14a2166

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:H/SI:L/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:P/AU:Y/R:X/V:C/RE:M/U:Red

EPSS: 0.000170000 probability, percentile 0.043200000 (date 2026-04-21)

Problem Types: CWE-522 | CWE-522 CWE-522: Insufficiently Protected Credentials

Version	Source	Type	Score	Severity	Vector
4.0	db4dfee8-a97e-4877-bfae-eba6d14a2166	Secondary	6.2	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N
4.0	CNA	CVSS	6.2	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:H/SI:L/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:P/AU:Y/R:X/V:C/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sparx Systems Pty Ltd.	Sparx Enterprise Architect	affected 16.1.1627	Not specified
CNA	Sparx Systems Pty Ltd.	Sparx Enterprise Architect	unaffected 17.1.1714	Not specified

References

Reference	Source	Link	Tags
sparxsystems.com/products/ea/17.1/history.html	db4dfee8-a97e-4877-bfae-eba6d14a2166	sparxsystems.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Pasi Orovuo, Solita Oy (en)

CNA: Henri Hämäläinen, Solita Oy (en)

CNA: Samu Ahvenainen, Solita Oy (en)

Additional Advisory Data

Solutions

CNA: Update to fixed version

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

Free CVE JSON API cve.report/api

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