



# Sparx Enterprise Architect Client reveals plaintext OAuth2 client secret

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

## Summary

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

## 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/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:C/RE:M/U:Re

**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/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/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:C/RE:M/U:Re
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/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/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:C/RE:M/U:Re

## 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/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:C/RE:M/U:Re  
d

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Sparx Systems Pty Ltd.</a>	<a href="#">Sparx Enterprise Architect</a>	affected 16.1.1627	Not specified
CNA	<a href="#">Sparx Systems Pty Ltd.</a>	<a href="#">Sparx Enterprise Architect</a>	unaffected 17.1.1714	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://sparxsystems.com/products/ea/17.1/history.html">sparxsystems.com/products/ea/17.1/history.html</a>	db4dfce8-a97e-4877-bfae-eba6d14a2166	<a href="https://sparxsystems.com">sparxsystems.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)