



Sparx Enterprise Architect Client does not verify the receiver of OAuth2 credentials during OpenID authentication

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

Summary

CVE	CVE-2025-15621
State	PUBLISHED
Assigner	NCSC-FI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 13:16:43 UTC
Updated	2026-04-17 15:17:00 UTC
Description	Insufficiently Protected Credentials in Sparx Systems Pty Ltd. Sparx Enterprise Architect. Client does not verify the receiver

Risk And Classification

Primary CVSS: v4.0 5.7 MEDIUM from db4dfee8-a97e-4877-bfae-eba6d14a2166

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:H/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:X

EPSS: 0.000170000 probability, percentile 0.042460000 (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	5.7	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:H/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:X
4.0	CNA	CVSS	5.7	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:H/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:X

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:H/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/MSI:X/MSA:X/S:P/AU:Y/R:X/V:C/RE:M/U:X

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.

© [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](#)