



# Unauthenticated execution of arbitrary SQL queries in Sparx Pro Cloud Server

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

## Summary

<b>CVE</b>	CVE-2025-15625
<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 09:16:04 UTC
<b>Updated</b>	2026-04-17 15:13:15 UTC
<b>Description</b>	Unauthenticated user is able to execute arbitrary SQL commands in Sparx Pro Cloud Server database in certain cases.

## Risk And Classification

**Primary CVSS:** v4.0 9.5 CRITICAL from db4dfee8-a97e-4877-bfae-eba6d14a2166

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:I/V:C/RE:M/U:R  
ed

**EPSS:** 0.000200000 probability, percentile 0.056140000 (date 2026-04-21)

**Problem Types:** CWE-89 | CWE-200 | CWE-89 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
4.0	db4dfee8-a97e-4877-bfae-eba6d14a2166	Secondary	9.5	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/V
4.0	CNA	CVSS	9.5	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/V

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:I/V:C/RE:M/U:R



### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sparx Systems Pty Ltd.	Sparx Pro Cloud Server	affected 6.0.163	Not specified

### References

Reference	Source	Link	Tags
sparxsystems.com/products/procloudserver/6.1/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, an



### Vendor Comments And Credit

Discovery Credit

**CNA:** Pasi Orovuo, Solita Oy (en)

**CNA:** Henri Hämäläinen, Solita Oy (en)

**CNA:** Samu Ahvenainen, Solita Oy (en)

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

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](#)