Sparx Pro Cloud Server reveals sensitive information to an unauthenticated user

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

Summary

CVE	CVE-2025-15623
State	PUBLISHED
Assigner	NCSC-FI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 09:16:04 UTC
Updated	2026-04-17 15:13:15 UTC
Description	Exposure of Private Personal Information to an Unauthorized Actor, : Exposure of Sensitive System Information to an Unau

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from db4dfee8-a97e-4877-bfae-eba6d14a2166

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:L/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: 0.000510000 probability, percentile 0.160810000 (date 2026-04-21)

Problem Types: CWE-359 | CWE-497 | CWE-359 CWE-359: Exposure of Private Personal Information to an Unauthorized Actor | CWE-497 CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

Version	Source	Type	Score	Severity	Vector
4.0	db4dfee8-a97e-4877-bfae-eba6d14a2166	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V/
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:L/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 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, ana

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.