Improper Enforcement of Disabled Accounts in WebUI SSO in Kiuwan SAST

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

Summary

CVE	CVE-2026-24069
State	PUBLISHED
Assigner	SEC-VLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 12:16:20 UTC
Updated	2026-04-14 19:16:33 UTC
Description	Kiuwan SAST improperly authorizes SSO logins for locally disabled mapped user accounts, allowing disabled users to cont

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from ADP

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

EPSS: 0.000170000 probability, percentile 0.040650000 (date 2026-04-14)

Problem Types: CWE-863 | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kiuwan	SAST	affected <2.8.2509.4	Not specified

References

Reference	Source	Link	Tags
r.sec-consult.com/kiuwanlock	551230f0-3615-47bd-b7cc-93e92e730bbf	r.sec-consult.com	
seclists.org/fulldisclosure/2026/Apr/5	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
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: Bernhard Gründling, SEC Consult Vulnerability Lab (en)

CNA: Fabian Würfl, SEC Consult Vulnerability Lab (en)

CNA: Johannes Greil, SEC Consult Vulnerability Lab (en)

Additional Advisory Data

Solutions

CNA: The issue was fixed for Kiuwan Cloud on 29 July 2025. For Kiuwan SAST on-premise (KOP), the issue is fixed in version 2.8.2509.4.

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**