



# CVE-2023-24724

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

## Summary

<b>CVE</b>	CVE-2023-24724
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-03 22:15:00 UTC
<b>Updated</b>	2023-11-07 04:08:00 UTC
<b>Description</b>	A stored cross site scripting (XSS) vulnerability was discovered in the user management module of the SAS 9.4 Admin Con

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sas	Web Administration Interface	9.4	m2	All	All

## References

Reference	Source
Stored XSS Vulnerability Discovered in SAS 9.4 Admin Console — CVE -2023-24724   by Willian AMORIM   Apr, 2023   Medium	
Stored XSS Vulnerability Discovered in SAS 9.4 Admin Console — CVE -2023-24724   by Willian AMORIM   Apr, 2023   Medium	MISC
Cross Site Scripting (XSS)   OWASP Foundation	MISC
55539 - The SAS® 9.4 Web Administration interface contains a cross-site scripting vulnerability.	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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](#)