



# CVE-2022-34298

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

## Summary

<b>CVE</b>	CVE-2022-34298
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-23 17:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	The NT auth module in OpenAM before 14.6.6 allows a "replace Samba username attack."

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openidentityplatform	Openam	All	All	All	All

## References

Reference	Source	Link
fix NT auth module vulnerability by maximthomas · Pull Request #514 · OpenIdentityPlatform/OpenAM · GitHub	MISC	<a href="#">github.com</a>
Release 14.6.6 · OpenIdentityPlatform/OpenAM · GitHub	MISC	<a href="#">github.com</a>
Comparing 14.6.5...14.6.6 · OpenIdentityPlatform/OpenAM · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)