



# CVE-2023-37471

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

## Summary

<b>CVE</b>	CVE-2023-37471
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-20 17:15:00 UTC
<b>Updated</b>	2023-07-31 18:44:00 UTC
<b>Description</b>	Open Access Management (OpenAM) is an access management solution that includes Authentication, SSO, Authorization,

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

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

## References

### Reference

User impersonation using SAMLv1.x SSO process. · Advisory · OpenIdentityPlatform/OpenAM · GitHub

GHSL-2023-143, GHSL-2023-144, deny unsigned SAML response by maximthomas · Pull Request #624 · OpenIdentityPlatform/OpenAM · GitHub

GHSL-2023-143, GHSL-2023-144, deny unsigned SAML response (#624) · OpenIdentityPlatform/OpenAM@7c18543 · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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

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