



# CVE-2023-32783

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-32783   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-08-07 17:15:00 UTC  |
| <b>Updated</b>         | 2024-03-14 16:15:00 UTC  |
| <b>Description</b>     | The event analysis component in Zoho ManageEngine ADAudit Plus 7.1.1 allows an attacker to bypass audit detection by c |

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product                  | Version | Update | Edition | Language |
|------------------|-----------|--------------------------|---------|--------|---------|----------|
| Operating System | Microsoft | Windows                  | -       | All    | All     | All      |
| Application      | Zohocorp  | Manageengine Aaudit Plus | 7.1.1   | All    | All     | All      |

## References

| Reference                                  | Source  | Link   | Tags                |
|--|---------|--|---------------------|
| ManageEngine ADAudit Plus (CVE-2023-32783) | MISC    | <a href="http://www.peteslade.com">www.peteslade.com</a> |                     |
| CVE Program record                         | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>             | canonical           |
| NVD vulnerability detail                   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>           | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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)