



# CVE-2017-1000501

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2017-1000501   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2018-01-03 15:29:00 UTC  |
| <b>Updated</b>         | 2020-07-27 03:15:00 UTC  |
| <b>Description</b>     | Awstats version 7.6 and earlier is vulnerable to a path traversal flaw in the handling of the "config" and "migrate" parameters. |

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                  | Product                      | Version | Update | Edition | Language |
|------------------|-------------------------|------------------------------|---------|--------|---------|----------|
| Application      | <a href="#">Awstats</a> | <a href="#">Awstats</a>      | All     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>  | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |

## References

| Reference  | Source  | Link  |
|--|---------|---|
| AWStats: Multiple vulnerabilities (GLSA 202007-37) — Gentoo security                                     | GENTOO  | <a href="https://security.gentoo.org">security.gentoo.org</a> |
| FIX Security reported by cPanel Security Team (can execute arbitrary · eldy/awstats@cf21984 · GitHub)    | CONFIRM | <a href="https://github.com">github.com</a>                   |
| [SECURITY] [DLA 1238-1] awstats security update  | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>       |
| AWStats - Open Source Log File Analyzer for advanced statistics (GNU GPL)                                | MISC    | <a href="https://www.awstats.org">www.awstats.org</a>         |
| Debian -- Security Information -- DSA-4092-1 awstats   | DEBIAN  | <a href="https://www.debian.org">www.debian.org</a>           |
| Fix another vulnerability reported by cPanel Security Team (can execute · eldy/awstats@06c0ab2 · GitHub) | CONFIRM | <a href="https://github.com">github.com</a>                   |
| CVE Program record   | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                 |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[198370](#) Ubuntu Security Notification for AWStats vulnerabilities (USN-4953-1)

[500043](#) Alpine Linux Security Update for awstats

[503725](#) Alpine Linux Security Update for awstats

[690578](#) Free Berkeley Software Distribution (FreeBSD) Security Update for awstats (4055aee5-f4c6-11e7-95f2-005056925db4)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)