



# CVE-2007-3949

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

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2007-3949                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2007-07-24 00:30:00 UTC                                                                                                       |
| <b>Updated</b>         | 2018-10-15 21:32:00 UTC                                                                                                       |
| <b>Description</b>     | mod_access.c in lighttpd 1.4.15 ignores trailing / (slash) characters in the URL, which allows remote attackers to bypass url |

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                   | Product                  | Version | Update | Edition | Language |
|-------------|--------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Lighttpd</a> | <a href="#">Lighttpd</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                       | Source  |
|---------------------------------------------------------------------------------------------------------------------------------|---------|
| Changeset 1871 - lighttpd - secure, fast, compliant, and very flexible web-server - Trac                                        | MISC    |
| Debian update for lighttpd - Advisories - Secunia                                                                               | SECUNIA |
| lighttpd 1.4.16 - Let's ship it                                                                                                 | CONFIRM |
| rPath update for lighttpd - Advisories - Secunia                                                                                | SECUNIA |
| Lighttpd Multiple Code Execution, Denial of Service and Information Disclosure Vulnerabilities                                  | BID     |
| lighttpd Multiple Vulnerabilities - Advisories - Secunia                                                                        | SECUNIA |
| SecurityFocus                                                                                                                   | BUGTRAQ |
| Gentoo update for lighttpd - Advisories - Secunia                                                                               | SECUNIA |
| #1230 (appending / to URL breaks access-deny setting) - lighttpd - secure, fast, compliant, and very flexible web-server - Trac | CONFIRM |
| Security Announcement                                                                                                           | SUSE    |
| Debian -- Security Information -- DSA-1362-2 lighttpd                                                                           | DEBIAN  |
| Gentoo Linux Documentation -- Lighttpd: Multiple vulnerabilities                                                                | GENTOO  |
| 38311                                                                                                                           | OSVDB   |

|                                                                                                                                          |         |
|------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                         | VUPEN   |
| CVE Program record                                                                                                                       | CVE.ORG |
| NVD vulnerability detail                                                                                                                 | NVD     |
| <div> <div></div> <div></div> </div>                                                                                                     |         |
| No vendor comments have been submitted for this CVE.                                                                                     |         |
| Legacy QID Mappings                                                                                                                      |         |
| <a href="#">690341</a> Free Berkeley Software Distribution (FreeBSD) Security Update for lighttpd (fc9c217e-3791-11dc-bb1a-000fea449b8a) |         |

© [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](#)