



CVE-2008-4360

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2008-4360 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2008-10-03 17:41:00 UTC |
| Updated | 2018-11-29 15:46:00 UTC |
| Description | mod_userdir in lighttpd before 1.4.20, when a case-insensitive operating system or filesystem is used, performs case-sensi |

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 4.0 | All | All | All |
| Operating System | Debian | Debian Linux | 4.0 | All | All | All |
| Application | Lighttpd | Lighttpd | All | All | All | All |
| Application | Lighttpd | Lighttpd | All | All | All | All |

References

| Reference | Source | Link |
|--|---------|--|
| Debian update for lighttpd - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| IBM X-Force Exchange | XF | exchange.xforce.ibmcloud.com |
| oss-security - Re: CVE request: lighttpd issues | MLIST | openwall.com |
| Redmine 404 error | CONFIRM | trac.lighttpd.net |
| Webmail OVH- OVH | VUPEN | www.vupen.com |
| rPath update for lighttpd - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| oss-security - Re: Re: CVE request: lighttpd issues | MLIST | openwall.com |
| Advisories:rPSA-2008-0309 - rPath Wiki | CONFIRM | wiki.rpath.com |
| Redmine 404 error | CONFIRM | trac.lighttpd.net |
| www.lighttpd.net/security/lighttpd_sa_2008_06.txt | CONFIRM | www.lighttpd.net |

| | | |
|--|---------|--|
| SUSE update for phpMyAdmin and lighttpd - Secunia.com | SECUNIA | secunia.com |
| oss-security - Re: CVE request: lighttpd issues | MLIST | openwall.com |
| SecurityFocus | BUGTRAQ | www.securityfocus.com |
| Debian -- Security Information -- DSA-1645-1 lighttpd | DEBIAN | www.debian.org |
| Lighttpd 'mod_userdir' Case Sensitive Comparison Security Bypass Vulnerability | BID | www.securityfocus.com |
| lighttpd: Multiple vulnerabilities — Gentoo Linux Documentation | GENTOO | security.gentoo.org |
| Lighttpd - Bug #1589: server.force-lowercase-filenames doesn't work inside userdir's - lighty labs | CONFIRM | trac.lighttpd.net |
| www.lighttpd.net/security/lighttpd-1.4.x_userdir_lowercase.patch | CONFIRM | www.lighttpd.net |
| Advisories:rPSA-2008-0309 - rPath Wiki | CONFIRM | wiki.rpath.com |
| lighttpd Weakness and Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| Security Advisory SA32972 - Gentoo update for lighttpd - Secunia | SECUNIA | secunia.com |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2008:026 | SUSE | lists.opensuse.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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

© 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](#).

CVE.report and Source URL Uptime Status status.cve.report