



CVE-2014-2469

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-2469
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-17 14:55:00 UTC
Updated	2016-06-02 02:24:00 UTC
Description	Unspecified vulnerability in lighttpd in Oracle Solaris 11.1 allows attackers to cause a denial of service via unknown vectors

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Sunos	5.11.1	All	All	All
Operating System	Oracle	Sunos	5.11.1	All	All	All

References

Reference	Source	Link
CVE-2014-2469 Denial of Service(DoS) vulnerability in Lighttpd Oracle Third Party Vulnerability Resolution Blog	CONFIRM	blogs.oracle.com
lighttpd Unspecified Bug Lets Remote Users Deny Service - SecurityTracker	SECTRACK	securitytracker.com
105298	OSVDB	www.osvdb.org
Malformed Request	BID	www.securityfocus.com
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](#)