



CVE-2012-5533

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

Summary

CVE	CVE-2012-5533
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-24 20:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	The http_request_split_value function in request.c in lighttpd before 1.4.32 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lighttpd	Lighttpd	1.4.31	All	All	All
Application	Lighttpd	Lighttpd	1.4.32	All	All	All
Application	Lighttpd	Lighttpd	1.4.31	All	All	All
Application	Lighttpd	Lighttpd	1.4.32	All	All	All

References

Reference	Source	Link
About Secunia Research Flexera	SECUNIA	secu
About Secunia Research Flexera	SECUNIA	secu
download.lighttpd.net/lighttpd/security/lighttpd-1.4.31_fix_connection_header_dos.p...	MISC	down
lighttpd 1.4.31 Denial of Service PoC	EXPLOIT-DB	www
Support / Security / Advisories // MDVSA-2013:100 Mandriva	MANDRIVA	www
Support/Advisories/MGASA-2012-0345 - Mageia wiki	CONFIRM	wiki.r
lighttpd 'http_request_split_value()' Function Remote Denial of Service Vulnerability	BID	www
Simple Lighttpd 1.4.31 Denial Of Service ~ Packet Storm	MISC	pack
openSUSE-SU-2012:1532-1: moderate: lighttpd	SUSE	lists.c
'[security bulletin] HPSBGN03191 rev.1 - HP Remote Device Access: Virtual Customer Access System (vCA' - MARC	HP	marc

openSUSE-SU-2014:0074-1: moderate: update for lighttpd to 1.4.32	SUSE	lists.c
download.lighttpd.net/lighttpd/security/lighttpd_sa_2012_01.txt	CONFIRM	down
IBM X-Force Exchange	XF	exch:
lighttpd Connection Header Processing Flaw Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www
87623	OSVDB	osvdl
oss-security - lighttpd 1.4.32 released, fixing CVE-2012-5533	MLIST	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

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](#)