



CVE-2013-4508

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

Summary

CVE	CVE-2013-4508
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-08 04:47:00 UTC
Updated	2021-02-26 15:11:00 UTC
Description	lighttpd before 1.4.34, when SNI is enabled, configures weak SSL ciphers, which makes it easier for remote attackers to hijack connections.

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Lighttpd	Lighttpd	All	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

References

Reference	Source	Link
oss-security - Re: CVE Request: lighttpd using vulnerable cipher suites with SNI	MLIST	openwa

download.lighttpd.net/lighttpd/security/lighttpd_sa_2013_01.txt	CONFIRM	download
Bug #2525: ssl.cipher-list not inherited into SNI - Lighttpd - lighty labs	CONFIRM	redmine
Debian -- Security Information -- DSA-2795-2 lighttpd	DEBIAN	www.de
Redmine 404 error	CONFIRM	redmine
JVN#37417423: Multiple vulnerabilities in SolarView Compact	JVN	jvn.jp
'[security bulletin] HPSBGN03191 rev.1 - HP Remote Device Access: Virtual Customer Access System (vCA' - MARC	HP	marc.inf
openSUSE-SU-2014:0072-1: moderate: update for lighttpd	SUSE	lists.ope
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

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](#)