



# CVE-2022-41556

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

## Summary

<b>CVE</b>	CVE-2022-41556
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-06 18:17:00 UTC
<b>Updated</b>	2023-11-07 03:52:00 UTC
<b>Description</b>	A resource leak in gw_backend.c in lighttpd 1.4.56 through 1.4.66 could lead to a denial of service (connection-slot exhaust

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Lighttpd</a>	<a href="#">Lighttpd</a>	All	All	All	All

## References

### Reference

- [Lighttpd: Denial of Service \(GLSA 202210-12\) — Gentoo security](#)
- [Comparing lighttpd-1.4.66...lighttpd-1.4.67 · lighttpd/lighttpd1.4 · GitHub](#)
- [\[SECURITY\] Fedora 35 Update: lighttpd-1.4.67-1.fc35 - package-announce - Fedora Mailing-Lists](#)
- [\[core\] handle RDHUP when collecting chunked body · b18de6f926 - lighttpd1.4 - Gitea: git hosting on git.lighttpd.net](#)
- [\[core\] release connections in CLOSE\\_WAIT & CON\\_STATE\\_READ\\_POST state by gmd20 · Pull Request #115 · lighttpd/lighttpd1.4 · GitHub](#)
- [\[SECURITY\] Fedora 35 Update: lighttpd-1.4.67-1.fc35 - package-announce - Fedora Mailing-Lists](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">181083</a> Debian Security Update for lighttpd (DSA 5243-1)
<a href="#">183019</a> Debian Security Update for lighttpd (CVE-2022-41556)
<a href="#">199198</a> Ubuntu Security Notification for lighttpd Vulnerabilities (USN-5903-1)
<a href="#">283176</a> Fedora Security Update for lighttpd (FEDORA-2022-c26b19568d)
<a href="#">502743</a> Alpine Linux Security Update for lighttpd
<a href="#">503685</a> Alpine Linux Security Update for lighttpd
<a href="#">710656</a> Gentoo Linux Lighttpd Denial of Service Vulnerability (GLSA 202210-12)

© [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](#)**