



CVE-2020-25691

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

Summary

CVE	CVE-2020-25691
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-01 23:15:00 UTC
Updated	2024-01-31 19:19:00 UTC
Description	A flaw was found in darkhttpd. Invalid error handling allows remote attackers to cause denial-of-service by accessing a file v

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Darkhttpd Project	Darkhttpd	All	All	All	All
Application	Unix4lyfe	Darkhttpd	All	All	All	All

References

Reference	Source
1893725 – (CVE-2020-25691) CVE-2020-25691 darkhttpd: sending an HTTP GET to a file with large modification date can cause a DoS	MITRE
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502558](#) Alpine Linux Security Update for darkhttpd

[503891](#) Alpine Linux Security Update for darkhttpd

[690977](#) Free Berkeley Software Distribution (FreeBSD) Security Update for darkhttpd (9c399521-5f80-11ed-8ac4-b42e991fc52e)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)