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

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)