



CVE-2021-45935

Published on: Not Yet Published

Last Modified on: 01/11/2022 06:54:00 PM UTC

CVE-2021-45935

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Grok](#) from [Grok Project](#) contain the following vulnerability:

Grok 9.5.0 has a heap-based buffer overflow in `openhjt2k::T1OpenHTJ2K::decompress` (called from

`std::__1::__packaged_task_func<std::__1::__bind<grk::T1DecompressScheduler::deco and std::__1::__packaged_task<int>).`

CVE-2021-45935 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
GitHub - osamu620/OpenHTJ2K: An open source implementation of	github.com	MISC github.com/osamu620/OpenHTJ2K

ITU-T Rec.814 | ISO 15444-15 (a.k.a. HTJ2K).

text/html

39021 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail

bugs.chromium.org

text/html

MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=39021

oss-fuzz-vulns/OSV-2021-1344.yaml at main · google/oss-fuzz-vulns · GitHub

github.com

text/html

MISC github.com/google/oss-fuzz-vulns/blob/main/vulns/grok/OSV-2021-1344.yaml

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

182943 Debian Security Update for libgrok2k (CVE-2021-45935)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grok Project	Grok	9.5.0	All	All	All

cpe:2.3:a:grok_project:grok:9.5.0:*****:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-45935 : Grok 9.5.0 has a heap-based buffer overflow in openhtj2k::T1OpenHTJ2K::decompress called from std... twitter.com/i/web/status/1...	2022-01-01 01:09:46