



# CVE-2021-42614

Published on: Not Yet Published

Last Modified on: 11/04/2022 04:45:00 PM UTC

## CVE-2021-42614

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

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A use after free in `info_width_internal` in `bk_info.c` in Halibut 1.2 allows an attacker to cause a segmentation fault or possibly have unspecified other impact via a crafted text document.

CVE-2021-42614 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

## CVE References

| Description                                                                               | Tags                                                                                          | Link                                                                                                                                                       |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Case Study: Security Analysis of Halibut - Carter Yagemann                                | <a href="https://carteryagemann.com/text/html">carteryagemann.com<br/>text/html</a>           | MISC <a href="https://carteryagemann.com/halibut-case-study.html#poc-halibut-info-uaf">carteryagemann.com/halibut-case-study.html#poc-halibut-info-uaf</a> |
| [SECURITY] Fedora 35 Update: halibut-1.3-3.fc35 - package-announce - Fedora Mailing-Lists | <a href="https://lists.fedoraproject.org/text/html">lists.fedoraproject.org<br/>text/html</a> | FEDORA <a href="https://lists.fedoraproject.org/archives/list/fedora@lists.fedoraproject.org/thread/9a9abd295b">FEDORA-2022-9a9abd295b</a>                 |

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](mailto:comment@cve.report).

## Related QID Numbers

[183956](#) Debian Security Update for halibut (CVE-2021-42614)

[282821](#) Fedora Security Update for halibut (FEDORA-2022-9a9abd295b)

## Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

## Known Affected Configurations (CPE V2.3)

| Type                                             | Vendor                          | Product                 | Version | Update | Edition | Language |
|--------------------------------------------------|---------------------------------|-------------------------|---------|--------|---------|----------|
| Operating System                                 | <a href="#">Fedoraproject</a>   | <a href="#">Fedora</a>  | 35      | All    | All     | All      |
| Application                                      | <a href="#">Halibut Project</a> | <a href="#">Halibut</a> | 1.2     | All    | All     | All      |
| cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:     |                                 |                         |         |        |         |          |
| cpe:2.3:a:halibut_project:halibut:1.2:*:*:*:*:*: |                                 |                         |         |        |         |          |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                   | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport | CVE-2021-42614 : A use after free in info_width_internal in bk_info.c in Halibut 1.2 allows an attacker to cause a... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-05-24 19:08:55 |
|  /r/netcve  | <a href="#">CVE-2021-42614</a>                                                                                                                                                                          | 2022-05-24 19:38:59 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)