



# CVE-2021-3575

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

## Summary

<b>CVE</b>	CVE-2021-3575
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-04 18:15:00 UTC
<b>Updated</b>	2023-02-12 23:41:00 UTC
<b>Description</b>	A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb when decompressing a crafted .j2

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	All	All	All	All

## References

Reference	Source
1957616 – (CVE-2021-3575) CVE-2021-3575 openjpeg: heap-buffer-overflow in color.c may lead to DoS or arbitrary code execution	MISC
Heap-buffer-overflow in color.c:379:42 in sycc420_to_rgb · Issue #1347 · uclouvain/openjpeg · GitHub	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
CVE-2021-3575   Ubuntu	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
[SECURITY] Fedora 33 Update: openjpeg2-2.3.1-11.fc33 - package-announce - Fedora Mailing-Lists	FEDOF
[SECURITY] Fedora 33 Update: openjpeg2-2.3.1-11.fc33 - package-announce - Fedora Mailing-Lists	MISC
[SECURITY] Fedora 34 Update: mingw-openjpeg2-2.4.0-3.fc34 - package-announce - Fedora Mailing-Lists	MISC

[SECURITY] Fedora 34 Update: mingw-openjpeg2-2.4.0-3.fc34 - package-announce - Fedora Mailing-Lists	FEDOF
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

159478 Oracle Enterprise Linux Security Update for openjpeg2 (ELSA-2021-4251)
239842 Red Hat Update for openjpeg2 (RHSA-2021:4251)
281630 Fedora Security Update for mingw (FEDORA-2021-e145f477df)
281631 Fedora Security Update for mingw (FEDORA-2021-c1ac2ee5ee)
353122 Amazon Linux Security Advisory for openjpeg2 : ALAS2-2022-1741
354833 Amazon Linux Security Advisory for openjpeg : ALAS2-2023-1999
502228 Alpine Linux Security Update for openjpeg
504233 Alpine Linux Security Update for openjpeg
940171 AlmaLinux Security Update for openjpeg2 (ALSA-2021:4251)
960346 Rocky Linux Security Update for openjpeg2 (RLSA-2021:4251)

© [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](#)