



# CVE-2020-35524

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

## Summary

<b>CVE</b>	CVE-2020-35524
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-09 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially cr

## 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="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	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

## References

Reference	Source	Link
tiff2pdf.c: properly calculate datasize when saving to JPEG YCbCr (7be2e452) · Commits · Oeronb / libtiff · GitLab	MISC	<a href="#">gitlab.com</a>
1932044 – (CVE-2020-35524) CVE-2020-35524 libtiff: Heap-based buffer overflow in TIFF2PDF tool	MISC	<a href="#">bugzilla.red</a>
[SECURITY] [DLA 2694-1] tiff security update	MLIST	<a href="#">lists.debian.</a>
Debian -- Security Information -- DSA-4869-1 tiff	DEBIAN	<a href="#">www.debiar</a>
[SECURITY] Fedora 33 Update: libtiff-4.1.0-8.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraq</a>
tiff2pdf.c: properly calculate datasize when saving to JPEG YCbCr (!159) · Merge Requests · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.com</a>

March 2021 LibTIFF Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.net</a>
libTIFF: Multiple vulnerabilities (GLSA 202104-06) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
[SECURITY] Fedora 33 Update: libtiff-4.1.0-8.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159477</a> Oracle Enterprise Linux Security Update for libtiff (ELSA-2021-4241)
<a href="#">178524</a> Debian Security Update for tiff (DSA 4869-1)
<a href="#">178685</a> Debian Security Update for tiff (DLA 2694-1)
<a href="#">199525</a> Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5841-1)
<a href="#">239810</a> Red Hat Update for libtiff (RHSA-2021:4241)
<a href="#">281368</a> Fedora Security Update for libtiff (FEDORA-2021-1bf4f2f13a)
<a href="#">296067</a> Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)
<a href="#">353264</a> Amazon Linux Security Advisory for libtiff : ALAS2-2022-1780
<a href="#">354038</a> Amazon Linux Security Advisory for libtiff : ALAS-2022-1625
<a href="#">501504</a> Alpine Linux Security Update for tiff
<a href="#">504473</a> Alpine Linux Security Update for tiff
<a href="#">670263</a> EulerOS Security Update for libtiff (EulerOS-SA-2021-1813)
<a href="#">670344</a> EulerOS Security Update for libtiff (EulerOS-SA-2021-1880)
<a href="#">670374</a> EulerOS Security Update for libtiff (EulerOS-SA-2021-1951)
<a href="#">670395</a> EulerOS Security Update for libtiff (EulerOS-SA-2021-1930)
<a href="#">710016</a> Gentoo Linux libTIFF Multiple Vulnerabilities (GLSA 202104-06)
<a href="#">751716</a> SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:0480-1)
<a href="#">751721</a> SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:0496-1)
<a href="#">751752</a> OpenSUSE Security Update for tiff (openSUSE-SU-2022:0480-1)
<a href="#">753222</a> SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:14888-1)
<a href="#">900105</a> CBL-Mariner Linux Security Update for libtiff 4.1.0

901841 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (6655-1)
902998 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (3963)
940061 AlmaLinux Security Update for libtiff (ALSA-2021:4241)
960705 Rocky Linux Security Update for libtiff (RLSA-2021:4241)

© [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](#)