



# CVE-2022-34526

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

## Summary

<b>CVE</b>	CVE-2022-34526
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-29 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:48:00 UTC
<b>Description</b>	A stack overflow was discovered in the _TIFFVGetField function of Tiffsplit v4.4.0. This vulnerability allows attackers to cau

## 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>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	4.4.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All

## References

Reference	Source
[SECURITY] Fedora 36 Update: libtiff-4.4.0-4.fc36 - package-announcement - Fedora Mailing-Lists	FEDOR
[SECURITY] Fedora 36 Update: libtiff-4.4.0-4.fc36 - package-announcement - Fedora Mailing-Lists	
CVE-2022-34526 LibTIFF Vulnerability in NetApp Products   NetApp Product Security	CONFIF
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN
tiffsplit: stack-buffer-overflow in _TIFFVGetField() (#433) · Issues · libtiff / libtiff · GitLab	MISC
tiffcrop: global-buffer-overflow in _TIFFVGetField(), another attack vector for CVE-2022-34526 (#486) · Issues · libtiff / libtiff · GitLab	MISC
[SECURITY] [DLA 3278-1] tiff security update	MLIST
CVE Program record	CVE.OF

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">181488</a> Debian Security Update for tiff (DLA 3278-1)
<a href="#">181520</a> Debian Security Update for tiff (DSA 5333-1)
<a href="#">182662</a> Debian Security Update for tiff (CVE-2022-34526)
<a href="#">199019</a> Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5714-1)
<a href="#">283016</a> Fedora Security Update for libtiff (FEDORA-2022-83b9a5bf0f)
<a href="#">354326</a> Amazon Linux Security Advisory for libtiff : ALAS2022-2022-194
<a href="#">354588</a> Amazon Linux Security Advisory for libtiff : ALAS-2022-194
<a href="#">355159</a> Amazon Linux Security Advisory for libtiff : ALAS2023-2023-050
<a href="#">502794</a> Alpine Linux Security Update for tiff
<a href="#">503030</a> Alpine Linux Security Update for tiff
<a href="#">503131</a> Alpine Linux Security Update for tiff
<a href="#">505944</a> Alpine Linux Security Update for tiff
<a href="#">672204</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2469)
<a href="#">672712</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1474)
<a href="#">672713</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1449)
<a href="#">672807</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1555)
<a href="#">672834</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1530)
<a href="#">672884</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1761)
<a href="#">672926</a> EulerOS Security Update for libtiff (EulerOS-SA-2023-1783)
<a href="#">752686</a> SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:3679-1)
<a href="#">752701</a> SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:3690-1)
<a href="#">902612</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10415)
<a href="#">902655</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10441)
<a href="#">903868</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10441-1)
<a href="#">903705</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10415-1)

© [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](#)**