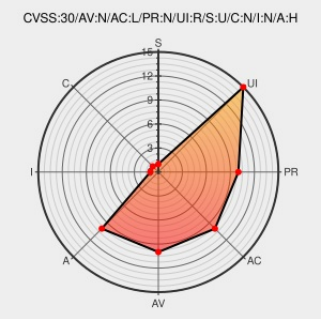
CVE-2018-5784

Published on: 01/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-5784

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

In LibTIFF 4.0.9, there is an uncontrolled resource consumption in the TIFFSetDirectory function of tif_dir.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tif file. This occurs because the declared number of directory entries is not validated against the actual number of directory entries.

CVE-2018-5784 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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
Bug 2772 – Uncontrolled resource consumption in TIFFSetDirectory (src/libtiff/tif_dir.c) (CVE-2018-5784)	Exploit Issue Tracking Third Party Advisory	MISC bugzilla.maptools.org/show_bug.cgi?id=2772

	bugzilla.maptools.org text/html	
USN-3602-1: LibTIFF vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3602-1
[SECURITY] [DLA 1411-1] tiff security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180702 [SECURITY] [DLA 1411-1] tiff security update
Fix for bug 2772 (473851d2) · Commits · libtiff / libtiff · GitLab	Patch Third Party Advisory gitlab.com text/html	CONFIRM gitlab.com/libtiff/libtiff/commit/473851d211cf8805a161820337ca74cc9615d6ef
[SECURITY] [DLA 1391-1] tiff security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180531 [SECURITY] [DLA 1391-1] tiff security update
Debian -- Security Information -- DSA-4349-1 tiff	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4349
USN-3606-1: LibTIFF vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3606-1

Related QID Numbers

500698 Alpine Linux Security Update for tiff

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libtiff	Libtiff	4.0.9	All	All	All
Application	Libtiff	Libtiff	4.0.9	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:4.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:libtiff:libtiff:4.0.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report