Bug 2074404 (CVE-2022-1354) - CVE-2022-1354 libtiff: heap-buffer-overflow in TIFFReadRawDataStriped() in tiffinfo.c

Keywords: Security ×

Status: NEW

Alias: CVE-2022-1354

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2075480 ~~2075479~~ 2075481 2075482 2075483

Blocks: 2074421 2075520

TreeView+ depends on / blocked

Reported: 2022-04-12 07:52 UTC by TEJ RATHI

Modified: 2022-11-15 10:35 UTC (History)

CC List: 18 users (show)

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: A heap buffer overflow flaw was found in Libtiffs' tiffinfo.c in TIFFReadRawDataStriped() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffinfo tool, triggering a heap buffer overflow issue and causing a crash that leads to a denial of service.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:8194	0	None	None	None	2022-11-15 10:35:27 UTC

TEJ RATHI 2022-04-12 07:52:29 UTC Description

A heap-buffer-overflow flaw was found in TIFFReadRawDataStriped() function in tiffinfo.c.

References:
https://gitlab.com/libtiff/libtiff/-/issues/319
https://gitlab.com/libtiff/libtiff/-/commit/87f580f39011109b3b
b5f6eca13fac543a542798

TEJ RATHI 2022-04-14 11:01:12 UTC Comment 3

Created libtiff tracking bugs for this issue:

Affects: fedora-all [~~bug 2075479~~]

Created mingw-libtiff tracking bugs for this issue:

Affects: fedora-all [bug 2075480]

errata-xmlrpc 2022-11-15 10:35:25 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2022:8194 https://access.redhat.com/errata/RHSA-
2022:8194