Bug 2074415 (CVE-2022-1355) - CVE-2022-1355 libtiff: stack-buffer-overflow in tiffcp.c in main()

Keywords: Security ×

Status: NEW

Alias: CVE-2022-1355

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2075489 ~~2075488~~ 2076189 2076190 2076191

Blocks: 2074421

TreeView+ depends on / blocked

Reported: 2022-04-12 08:04 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 stack buffer overflow flaw was found in Libtiffs' tiffcp.c in main() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffcp tool, triggering a stack buffer overflow issue, possibly corrupting the memory, 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-2022:7585	0	None	None	None	2022-11-08 09:45:27 UTC
Red Hat Product Errata	RHSA-2022:8194	0	None	None	None	2022-11-15 10:35:30 UTC

TEJ RATHI 2022-04-12 08:04:58 UTC Description

A stack-buffer-overflow flaw was found in tiffcp.c in main()

References:
https://gitlab.com/libtiff/libtiff/-/issues/400
https://gitlab.com/libtiff/libtiff/-/merge_requests/323

TEJ RATHI 2022-04-14 11:12:16 UTC Comment 2

Created libtiff tracking bugs for this issue:

Affects: fedora-all [~~bug 2075488~~]

Created mingw-libtiff tracking bugs for this issue:

Affects: fedora-all [bug 2075489]

errata-xmlrpc 2022-11-08 09:45:24 UTC Comment 6

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2022:7585 https://access.redhat.com/errata/RHSA-2022:7585

errata-xmlrpc 2022-11-15 10:35:29 UTC Comment 7

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