Bug 1939233 (CVE-2021-3443) - CVE-2021-3443 jasper: NULL pointer dereference in jp2_decode() in jp2_dec.c

Keywords: Security ×

Status: NEW

Alias: CVE-2021-3443

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: 🔒 1941824 🔒 1943628 ~~1939240~~ ~~1939241~~ 🔒 1941825 🔒 1941826 🔒 1943627

Blocks: 🔒 1939236 🔒 1939237

TreeView+ depends on / blocked

Reported: 2021-03-15 19:13 UTC by Guilherme de Almeida Suckevicz

Modified: 2022-04-17 21:13 UTC (History)

CC List: 7 users (show)

Fixed In Version: jasper 2.0.27

Doc Type: If docs needed, set a value

Doc Text:

```
A NULL pointer dereference flaw was found in the
way Jasper versions before 2.0.27 handled
component references in the JP2 image format
decoder. A specially crafted JP2 image file could
cause an application using the Jasper library to
crash when opened.
```

Clone Of:

Environment:

Last Closed:

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

Guilherme de Almeida Suckevicz 2021-03-15 19:13:15 UTC Description

```
A flaw was found in jasper before 2.0.26. A NULL pointer dereference in jp2_decode in jp2_dec.c may lead to program crash and denial of service.

Reference:
https://github.com/jasper-software/jasper/issues/269

Upstream patch:
https://github.com/jasper-software/jasper/commit/f94e7499a8b1471a4905c4f9c9e12e60fe88264b
```

Guilherme de Almeida Suckevicz 2021-03-15 19:27:08 UTC Comment 1

```
Created jasper tracking bugs for this issue:

Affects: fedora-all [ bug 1939240 ]


Created mingw-jasper tracking bugs for this issue:

Affects: fedora-all [ bug 1939241 ]
```

Tomas Hoger 2021-03-22 21:12:18 UTC Comment 4

```
In reply to comment #0:
> A flaw was found in jasper before 2.0.26.

The "before" here is incorrect - it was reported in 2.0.26, and fixed in 2.0.27.
```

Tomas Hoger 2021-03-23 16:30:25 UTC Comment 6

```
Note that the fist Jasper version that crashes with the reproducer included in the upstream bug report is 2.0.20.  However, the problem exists in earlier
versions as well.  More detailed analysis can be found in the upstream issue:

https://github.com/jasper-software/jasper/issues/269#issuecomment-804423097
```

Note
You need to log in before you can comment on or make changes to this bug.