Bug 2074549 (CVE-2022-1325) - CVE-2022-1325 CImg: Denial of service via RAM exhaustion in _load_bmp

Keywords:	Security ×
Status:	CLOSED UPSTREAM
Alias:	CVE-2022-1325
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:	2074550
Blocks:	2074551
TreeView+	depends on / blocked

Reported:	2022-04-12 13:24 UTC by Pedro Sampaio
Modified:	2022-04-22 18:24 UTC (History)
CC List:	2 users (show)
Fixed In Version:	
Doc Type:	If docs needed, set a value
Doc Text:	
Clone Of:	
Environment:	
Last Closed:	2022-04-12 15:26:39 UTC

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

Pedro Sampaio 2022-04-12 13:24:51 UTC Description

```
In CImg 3.10, via a maliciously crafted bmp file with modified
dx and dy header field values it is possible to trick the
application into allocating huge buffer sizes like 64 Gigabyte
upon reading the file from disk or from a virtual buffer.

Upstream issue:

https://github.com/dtschump/CImg/issues/343
```

Pedro Sampaio 2022-04-12 13:25:52 UTC Comment 1

Created CImg tracking bugs for this issue:

Affects: fedora-all [bug 2074550]

Product Security DevOps Team 2022-04-12 15:26:37 UTC Comment 2

This CVE Bugzilla entry is for community support informational purposes only as it does not affect a package in a commercially supported Red Hat product. Refer to the dependent bugs for status of those individual community products.

Pedro Sampaio 2022-04-22 18:24:33 UTC Comment 3

Upstream fix:

https://github.com/dtschump/cimg/commit/619cb58dd90b4e03ac68286c70ed98acbefd1c90