Bug 1946289 (CVE-2021-20308) - CVE-2021-20308 htmldoc: Integer overflow in image_load_gif()

Keywords: Security ×

Status: CLOSED UPSTREAM
Alias: CVE-2021-20308
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: 1946291 ~~1946290~~
Blocks: 1946292
TreeView+ depends on / blocked

Reported: 2021-04-05 17:36 UTC by Pedro Sampaio
Modified: 2021-04-06 19:04 UTC (History)
CC List: 2 users (show)
Fixed In Version:
Doc Type: If docs needed, set a value
Doc Text: An integer overflow flaw was found in HTMLDOC. This flaw allows attackers to execute arbitrary code and cause a denial of service. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-04-05 23:35:14 UTC

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

Pedro Sampaio 2021-04-05 17:36:20 UTC — Description

Integer overflow in the htmldoc 1.9.11 and before may allow attackers to execute arbitrary code and cause a denial of service that is similar to CVE-2017-9181.

Upstream bug:

https://github.com/michaelrsweet/htmldoc/issues/423

Pedro Sampaio 2021-04-05 17:36:51 UTC — Comment 1

Created htmldoc tracking bugs for this issue:

Affects: epel-7 [bug 1946291]
Affects: fedora-all [~~bug 1946290~~]

Product Security DevOps Team 2021-04-05 23:35:14 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.

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