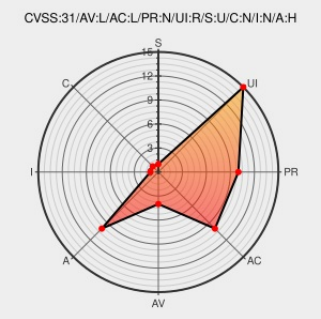
CVE-2022-1325

Published on: Not Yet Published

Last Modified on: 02/12/2023 10:10:54 PM UTC

CVE-2022-1325

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cimg from Cimg contain the following vulnerability:

A flaw was found in CImg, where with the help of a maliciously crafted pandore or 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.

CVE-2022-1325 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
2074549 – (CVE-2022-1325) CVE-2022-1325 CImg: Denial of service via RAM exhaustion in _load_bmp	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2074549
Denial of service via RAM exhaustion in _load_bmp · Issue #343 · GreycLab/CImg · GitHub	github.com text/html	MISC github.com/GreycLab/CImg/issues/343
CImg<>::load_bmp() and CImg<>::load_pandore(): Check that dimensions … · GreycLab/CImg@619cb58 · GitHub	github.com text/html	MISC github.com/GreycLab/CImg/commit/619cb58dd90b4e03ac68286c70ed98acbefd1c90
add global hardening against	github.com	MISC github.com/GreycLab/CImg/pull/348

RAM exhaustions in safe_size by 7unn3l · Pull Request #348 · GreycLab/CImg · GitHub	text/html	
unchecked size in _load_bmp leads to RAM exhaustion in version 3.10 vulnerability found in cimg	huntr.dev text/html	MISC huntr.dev/bounties/a5e4fc45-8f14-4dd1-811b-740fc50c95d2/
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2022-1325

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

182019 Debian Security Update for cimg (CVE-2022-1325)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cimg	Cimg	All	All	All	All

cpe:2.3:a:cimg:cimg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-1325 : A flaw was found in CImg, where with the help of a maliciously crafted pandore or bmp file with mod… twitter.com/i/web/status/1…	2022-08-31 16:06:27

← Previous ID

Next ID→