

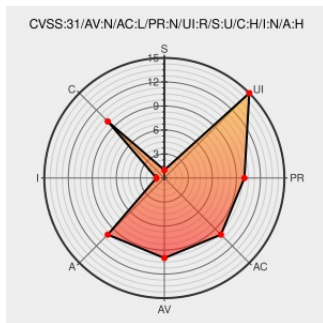


CVE-2020-25693

Published on: 12/03/2020 12:00:00 AM UTC

Last Modified on: 05/05/2021 01:06:00 PM UTC

CVE-2020-25693

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cimg](#) from [Cimg](#) contain the following vulnerability:

A flaw was found in Cimg in versions prior to 2.9.3. Integer overflows leading to heap buffer overflows in load_pnm() can be triggered by a specially crafted input file processed by Cimg, which can lead to an impact to application availability or data integrity.

CVE-2020-25693 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 33 Update: gmic-2.9.7-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-ca1151e997
[SECURITY] Fedora 32 Update: gmic-2.9.7-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-bc6585e31a

1893377 – (CVE-2020-25693) CVE-2020-25693 Cimg: multiple integer overflows leading to heap-based buffer-overflows

Exploit

Issue Tracking

Patch

Third Party Advisory

bugzilla.redhat.com

text/html

MISC

bugzilla.redhat.com/show_bug.cgi?id=1893377

[SECURITY] Fedora 34 Update: Cimg-2.9.7-1.fc34 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org

text/html

FEDORA

FEDORA-2021-2aaba884af

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

281700

Fedora Security Update for Cimg (FEDORA-2021-2aaba884af)

281701

Fedora Security Update for Cimg (FEDORA-2021-ca1151e997)

281702

Fedora Security Update for Cimg (FEDORA-2021-bc6585e31a)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cimg	Cimg	All	All	All	All
Application	Cimg	Cimg	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
cpe:2.3:a:cimg:cimg:*****:.*						
cpe:2.3:a:cimg:cimg:*****:.*						
cpe:2.3:o:fedoraproject:fedora:32:*****:.*						
cpe:2.3:o:fedoraproject:fedora:33:*****:.*						
cpe:2.3:o:fedoraproject:fedora:34:*****:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)