

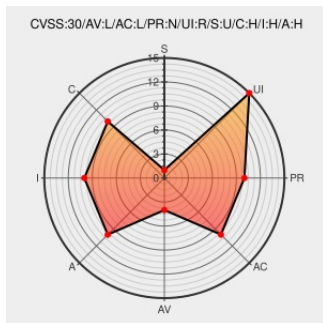


CVE-2018-7588

Published on: 03/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-7588

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

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

An issue was discovered in Cimg v.220. A heap-based buffer over-read in load_bmp in Cimg.h occurs when loading a crafted bmp image.

CVE-2018-7588 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 1934-1] cimg security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20190928 [SECURITY] [DLA 1934-1] cimg security update
[SECURITY] [DLA 2421-1] cimg security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20201030 [SECURITY] [DLA 2421-1] cimg security update

USN-4039-1: CImg vulnerabilities | Ubuntu security notices | Ubuntu

usn.ubuntu.com
text/html

UBUNTU USN-4039-1

a heap overflow when load a bmp image · Issue #183 · dtschump/CImg · GitHub

Third Party Advisory
github.com
text/html

MISC github.com/dtschump/CImg/issues/183

pocs/cimg at master · xiaoqx/pocs · GitHub

Exploit
Third Party Advisory
github.com
text/html

MISC github.com/xiaoqx/pocs/tree/master/cimg

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cimg	Cimg	.220	All	All	All
Application	Cimg	Cimg	.220	All	All	All
cpe:2.3:a:cimg:cimg:.220:*****:						
cpe:2.3:a:cimg:cimg:.220:*****:						

No vendor comments have been submitted for this CVE