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

Keywords: Security ×

Status: CLOSED UPSTREAM
Alias: CVE-2020-25693
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: ~~1893378~~
Blocks: 1893312
TreeView+ depends on / blocked

Reported: 2020-10-30 22:34 UTC by Todd Cullum
Modified: 2021-02-10 14:07 UTC (History)
CC List: 2 users (show)
Fixed In Version: CImg 2.9.3
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in the CImg library. Multiple integer overflows lead to heap buffer overflows in load_pnm(), which can be triggered by a specially crafted input file processed by CImg. The highest risk from this vulnerability is to integrity and system availability.
Clone Of:
Environment:
Last Closed: 2020-10-31 02:21:14 UTC

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

Todd Cullum 2020-10-30 22:34:05 UTC — Description

The CImg.h image library uses an unsafe pattern that is prone to integer overflows to calculate the required heap buffer allocation size. The resulting small heap buffers can be trivially overwritten by a malformed image input. This has been demonstrated at least with the load_pnm() image parsing function.

References:
https://github.com/dtschump/CImg/pull/295
https://bugs.launchpad.net/ubuntu/+source/cimg/+bug/1900983

Todd Cullum 2020-10-30 22:34:08 UTC — Comment 1

Acknowledgments:

Name: Kai Dietrich

Todd Cullum 2020-10-30 22:34:19 UTC — Comment 2

Created CImg tracking bugs for this issue:

Affects: fedora-all [~~Bug 1893378~~]

Product Security DevOps Team 2020-10-31 02:21:14 UTC — Comment 3

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.

Todd Cullum 2020-11-03 19:13:29 UTC — Comment 4

Upstream commit: https://github.com/dtschump/CImg/pull/295/commits/4f184f89f9ab6785a6c90fd238dbaa6d901d3505

Todd Cullum 2020-11-03 19:23:17 UTC — Comment 5

Flaw summary:

In CImg.h, the pattern `(size_t)size_x*size_y*size_z*size_c` is used in multiple locations but it was discovered that it can wrap (called "overflow" in the commit) the resulting `size_t` value. The patch introduces a function called `_safe_size()` which performs the calculations whilst preventing unsigned integer wrap in the result.

Because the above calculations are used in allocation of heap memory, the flaw can lead to arbitrary heap memory write in subsequent code when specially crafted input is provided to CImg. It is more likely to occur on platforms where the `size_t` type is 32-bit.

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