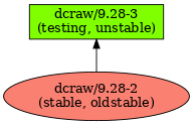
Debian Bug report logs - #984761

dcraw: CVE-2021-3624: buffer-overflow caused by integer-overflow in foveon_load_camf()



Package: dcraw; Maintainer for dcraw is Debian Astronomy Team <debian-astro-maintainers@lists.alioth.debian.org>; Source for dcraw is src:dcraw (PTS, buildd, popcon).

Reported by: Wooseok Kang <kangwoosuk1@gmail.com>

Date: Mon, 8 Mar 2021 04:42:02 UTC

Severity: normal

Tags: security, upstream

Found in version dcraw/9.28-2

Fixed in version dcraw/9.28-3

Done: Filip Hroch <hroch@physics.muni.cz>

Bug is archived. No further changes may be made.

Toggle useless messages

View this report as an mbox folder, status mbox, maintainer mbox

---

Message #5 received at submit@bugs.debian.org (full text, mbox, reply):

From: Wooseok Kang <kangwoosuk1@gmail.com>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: dcraw: buffer-overflow caused by integer-overflow in foveon_load_camf()
Date: Mon, 08 Mar 2021 13:37:46 +0900

[Message part 1 (text/plain, inline)]

```
Package: dcraw

Version: 9.28-2

Severity: normal

X-Debbugs-Cc: kangwoosuk1@gmail.com


Dear Maintainer,


There is an integer overflow vulnerability in dcraw.

When the victim runs dcraw with a maliciously crafted X3F input image,

arbitrary code may be executed in the victim's system.


The vulnerability resides in foveon_load_camf() function in dcraw.c file.

The program reads data from the input image using get4().


type = get4();  get4();  get4();

wide = get4();

high = get4();


Since there is no sanitization for these variables, we can set their values freely.

Let type=4, and wide and high are enough large values which can make overflow.

Then, it will lead to small memory allocation at the below code.


} else if (type == 4) {

    free (meta_data);

    meta_length = wide*high*3/2;

    meta_data = (char *) malloc (meta_length);


Therefore, when we read data to this allocated buffer,

it causes the buffer overrun which may lead to arbitrary code execution or program crash.
```

I attach the maliciously crafted X3F file which crashes dcraw like below.

> dcraw dcraw-poc.X3F

dcraw-poc.X3F: Corrupt data near 0x651

[1]   1251 segmentation fault dcraw dcraw-poc.X3F

Thank you.

-- System Information:

Debian Release: bullseye/sid

  APT prefers testing

  APT policy: (500, 'testing')

Architecture: amd64 (x86_64)

Kernel: Linux 5.4.72-microsoft-standard-WSL2 (SMP w/16 CPU threads)

Locale: LANG=en_US.UTF-8, LC_CTYPE=en_US.UTF-8 (charmap=UTF-8), LANGUAGE not set

Shell: /bin/sh linked to /bin/dash

Init: unable to detect

Versions of packages dcraw depends on:

ii libc6   2.31-9

ii libjpeg62-turbo 1:2.0.6-2

ii liblcms2-2   2.12~rc1-2

dcraw recommends no packages.

Versions of packages dcraw suggests:

pn gphoto2 <none>

pn netpbm   <none>

-- no debconf information

[dcraw-poc.X3F (image/x-x3f, attachment)]

Message #10 received at 984761@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Filip Hroch <hroch@physics.muni.cz>
To: 984761@bugs.debian.org
Subject: dcraw: buffer-overflow caused by integer-overflow in foveon_load_camf()
Date: Tue, 09 Mar 2021 17:41:51 +0100

Dear Wooseok,

I'll look on this.

Note, that I'm maintaining only Debian packaging.

I am not upstream autor; I can fix only the bugs

which does not induce extensive changes in whole

structure of the source code.

FH

--

F. Hroch <hroch@physics.muni.cz>, Masaryk University, Brno,

Czechia.

Dept. of theor. physics and astrophysics, Kotlarska 2, CZ-611 37.

Added tag(s) security. Request was from Adrian Bunk <bunk@debian.org> to control@bugs.debian.org. (Mon, 31 May 2021 20:51:02 GMT) (full text, mbox, link).

Message #17 received at 984761@bugs.debian.org (full text, mbox, reply):

From: Salvatore Bonaccorso <carnil@debian.org>
To: Filip Hroch <hroch@physics.muni.cz>, 984761@bugs.debian.org, 984761-submitter@bugs.debian.org
Subject: Re: Bug#984761: dcraw: buffer-overflow caused by integer-overflow in foveon_load_camf()
Date: Wed, 2 Jun 2021 22:40:19 +0200

Hi Filip, Wooseok

On Tue, Mar 09, 2021 at 05:41:51PM +0100, Filip Hroch wrote:

> Dear Wooseok,
>
> I'll look on this.
>
> Note, that I'm maintaining only Debian packaging.
> I am not upstream autor; I can fix only the bugs
> which does not induce extensive changes in whole
> structure of the source code.

Can you please report the issue upstream? Or was this reported
upstream?

Regards,
Salvatore

Message sent on to Wooseok Kang <kangwoosuk1@gmail.com>:

Bug#984761. (Wed, 02 Jun 2021 20:42:07 GMT) (full text, mbox, link).

Message #25 received at 984761@bugs.debian.org (full text, mbox, reply):

From: Filip Hroch <hroch@physics.muni.cz>
To: Salvatore Bonaccorso <carnil@debian.org>
Cc: 984761@bugs.debian.org, 984761-submitter@bugs.debian.org
Subject: Re: Bug#984761: dcraw: buffer-overflow caused by integer-overflow in foveon_load_camf()
Date: Thu, 03 Jun 2021 12:35:21 +0200

Dear Salvatore,

unfortunatelly, I have not fixed it yet.

I suppose to report it to upstream author -- Mr. Coffin.
In past, I send patches without any response.

The last upstream version of dcraw has been issued
tree years ago, so I've some worry about him.

Regards,
FH

Salvatore Bonaccorso <carnil@debian.org> writes:

> Hi Filip, Wooseok

>

> On Tue, Mar 09, 2021 at 05:41:51PM +0100, Filip Hroch wrote:

>> Dear Wooseok,

>>

>> I'll look on this.

>>

>> Note, that I'm maintaining only Debian packaging.

>> I am not upstream autor; I can fix only the bugs

>> which does not induce extensive changes in whole

>> structure of the source code.

>

> Can you please report the issue upstream? Or was this reported

> upstream?

>

> Regards,

> Salvatore

--

F. Hroch <hroch@physics.muni.cz>, Masaryk University,

Dept. of theor. physics and astrophysics, Brno, Moravia, CZ

Message sent on to Wooseok Kang <kangwoosuk1@gmail.com>:

Bug#984761. (Thu, 03 Jun 2021 10:45:06 GMT) (**full text**, **mbox**, **link**).

Changed Bug title to 'dcraw: CVE-2021-3624: buffer-overflow caused by integer-overflow in foveon_load_camf()' from 'dcraw: buffer-overflow caused by integer-overflow in foveon_load_camf()'. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Tue, 29 Jun 2021 05:45:05 GMT) (**full text**, **mbox**, **link**).

Reply sent to Filip Hroch <hroch@physics.muni.cz>:

You have taken responsibility. (Thu, 25 Nov 2021 13:06:14 GMT) (**full text**, **mbox**, **link**).

Message #35 received at 984761-close@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Debian FTP Masters <ftpmaster@ftp-master.debian.org>
To: 984761-close@bugs.debian.org
Subject: Bug#984761: fixed in dcraw 9.28-3
Date: Thu, 25 Nov 2021 13:03:53 +0000

Source: dcraw

Source-Version: 9.28-3

Done: Filip Hroch <hroch@physics.muni.cz>

We believe that the bug you reported is fixed in the latest version of

dcraw, which is due to be installed in the Debian FTP archive.

A summary of the changes between this version and the previous one is

attached.

Thank you for reporting the bug, which will now be closed. If you

have further comments please address them to 984761@bugs.debian.org,

and the maintainer will reopen the bug report if appropriate.

Debian distribution maintenance software

pp.

Filip Hroch <hroch@physics.muni.cz> (supplier of updated dcraw package)

(This message was generated automatically at their request; if you

believe that there is a problem with it please contact the archive

administrators by mailing ftpmaster@ftp-master.debian.org)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Format: 1.8

Date: Sun, 21 Nov 2021 23:15:39 +0100

Source: dcraw

Architecture: source

Version: 9.28-3

Distribution: unstable

Urgency: medium

Maintainer: Debian Astronomy Team <debian-astro-maintainers@lists.alioth.debian.org>

Changed-By: Filip Hroch <hroch@physics.muni.cz>

Closes: 478701 914447 914453 914454 914459 984761

Changes:

 dcraw (9.28-3) unstable; urgency=medium

 .

   * Written wrappers of fread(),fwrite(),fseek() library functions which

     checks their return values. If an input/output failure is detected,

     dcraw immediately exits with non-zero status and prints a descriptive

     message. Closes: #478701, #914447, #914453, #914454, #914459, #984761

   * Updated links; upstream has been moved to a new site.

   * Updated packaging: evolving standards, added metadata, lintian.

Checksums-Sha1:

 25dc6466c9400cbb583545d7ee4311352286ad05 1978 dcraw_9.28-3.dsc

 cb2b167a49544b5bf879d4a2ef8970b9390b0631 6865640 dcraw_9.28-3.debian.tar.xz

Checksums-Sha256:

 9927b846c8f93188ae84bcd7831d6d61bc83561dba7ba2440b6dafd18ca4b74d 1978 dcraw_9.28-3.dsc

 357ef76c9ad7c0f16f12a29d81a1dc3ee8dff1099c30636fc38fb4109f6a3db6 6865640 dcraw_9.28-3.debian.tar.xz

Files:

 da4d8776a65a9ac1e37c5ee6a272fd5b 1978 graphics optional dcraw_9.28-3.dsc

 d05b8ef6e95acc707c5d43b82bb9ee02 6865640 graphics optional dcraw_9.28-3.debian.tar.xz

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEuvxshffLFD/utvsVcRWv0HcQ3PcFAmGfguIACgkQcRWv0HcQ

3PfJLg/+McreFSi3qAg/tpwPYNMXhrQIrhK3KaCdQaJFxkTajhI2j9MeESE4UZYk

VluDMqtcvbUJP9vSCQDr9z2q66h4u877ckI3nys/ueNKSQM5NRyTcWjzuqCMZdSz

0LZ6qO/UftRIn3HxYWWYZDgO+36I7u5Ua4wPNm+dYCqNED2sALK3sZKBd2WiVfhE

HMbHnpiMLwPVCO4RUVGluDht0fsHPaV4rPEo0JPvipwHnpgrAKcGP55r+5EGbPdL

HuTahEDiZKhl4MBIEVHAuC2wN8HPhTpONhxIvDbrQm/HLIwm/XPt/N9QTXbv0miW

b204OoXkT33LP8eRz+U3tDpGxQU/dnEZ05sClfV+85n1Tw9Atzle/tqyeg8dVscv

jUmCu10q3ESubpnU4Opdxcm5qt5QB59z6gFnd5wzyaVQehRcGg/luUaeneqguWxz

U82aiwosXEmioXPYeDAzmkjULDliguwAnSx6BNVGzf/t3XReVW07bFXsnpT8XASc

0LzzKA3Mzjt0y8UM9YvV9vs0SIXuxWLQa5WUfK41TGlwza8wBMewuUQJ2+r161mG

mYrXb2vz8/8nU2jz+RdUQvhYXSWrRaiQ3Vj+Qcx8eSrveaCLM8RZqgKf6m6STev5

zIz4iwhJZVz78n+M2aci/tjZ+Fhr9RLCuZRDakQFOv5Cq5XzJJk=

=3QxF

-----END PGP SIGNATURE-----

Bug archived. Request was from Debbugs Internal Request <owner@bugs.debian.org> to internal_control@bugs.debian.org. (Sat, 25 Dec 2021 07:29:15 GMT) (**full text**, **mbox**, **link**).

Bug unarchived. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Wed, 13 Apr 2022 05:00:02 GMT) (**full text**, **mbox**, **link**).

Added tag(s) upstream. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Wed, 13 Apr 2022 05:00:03 GMT) (**full text**, **mbox**, **link**).

Bug archived. Request was from Debbugs Internal Request <owner@bugs.debian.org> to internal_control@bugs.debian.org. (Wed, 11 May 2022 07:27:12 GMT) (**full text**, **mbox**, **link**).

Send a report that **this bug log contains spam**.
