New issue

Jump to bottom

OpenDMARC 1.4.1 segfault several times on two VMs, CentOS 7/8 #179

Closed cseres3 opened this issue on Jun 8, 2021 · 28 comments

Assignees

cseres3 commented on Jun 8, 2021 • edited

Hi,
yesterday and today OpenDMARC has crashed for segfault half a dozen times on two virtual machines, one of them CentOS7, another CentOS8, both up-to-date and have OpenDKIM version 1.4.1. Before yesterday OpenDMARC and libopendmarc version 1.3.2 was installed and they worked fine.

Last dmesg info was

```
[Tue Jun 8 11:19:32 2021] opendmarc[11107]: segfault at 0 ip 00007fa89690c327 sp 00007fa88ffdb1a8 error 4 in libc-2.17.so[7fa8967c5000+1c4000]
```

Red Hat Abrtd service was running, there is coredump and other files saved by it. Is there some additional information you would need to investigate the issue?

The package version is opendmarc-1.4.1-1.el7.x86_64 on CentOS7 and opendmarc-1.4.1-1.el8.x86_64 on CentOS8.

glts commented on Jun 8, 2021 Contributor

Please provide the backtrace from the coredump.

cseres3 commented on Jun 8, 2021 • edited Author

backtrace.txt
Backtrace created with abrt-action-generate-backtrace attached. One name is replaced with xx's.

glts commented on Jun 8, 2021 Contributor

I have difficulties deciphering this, but if I had to go out on a limb this looks like a NULL dereference here: https://github.com/trusteddomainproject/OpenDMARC/blob/rel-opendmarc-1-4-1/opendmarc/opendmarc.c#L2480

This is the fix for CVE-2019-16378. If OpenDMARC can now be crashed with a multi-value `From` input then that fix just opened a new hole (DoS). Would be good to have a repro. Then someone file a new CVE if necessary ...

sriccio commented on Jun 9, 2021 • edited

Hello,

We're seeing the same issue here on E.F.A v4.

opendmarc packages were updated and it started to segfault daily at random times

```
[root@mx1 ~]# yum history info 136
Loaded plugins: fastestmirror
Transaction ID : 136
Begin time     : Mon Jun  7 08:43:36 2021
Begin rpmdb    : 750:3e7c4467092ba328515d976ae9be6ab76f463611
End time       :            08:43:38 2021 (2 seconds)
End rpmdb      : 750:edee20cdba2ea3ea406f889beea1a52f367411ac
User           : root <root>
Return-Code    : Success
Transaction performed with:
    Installed     rpm-4.11.3-45.el7.x86_64                      @base
    Installed     yum-3.4.3-168.el7.centos.noarch               @base
    Installed     yum-metadata-parser-1.1.4-10.el7.x86_64       @anaconda
    Installed     yum-plugin-fastestmirror-1.1.31-54.el7_8.noarch @updates
Packages Altered:
    Updated libopendmarc-1.3.2-1.el7.x86_64 @epel
    Update              1.4.1-1.el7.x86_64 @epel
    Updated opendmarc-1.3.2-1.el7.x86_64    @epel
    Update            1.4.1-1.el7.x86_64    @epel


[92878.213379] opendmarc[16670]: segfault at 0 ip 00007f501d31b2a1 sp 00007f4fd97d61a8 error 4 in libc-2.17.so[7f501d1d4000+1c4000]
```

I've considered a rollback to 1.3.2-1.el7.x86_64 but the files seems gone from EPEL directories...

glts commented on Jun 9, 2021 • edited Contributor

I could reproduce the problem and have pushed another commit at #178. Please apply and try patch https://patch-diff.githubusercontent.com/raw/trusteddomainproject/OpenDMARC/pull/178.patch.

Please someone file a CVE, I don't have the energy right now. OpenDMARC 1.4.1.1 is a sitting duck and can be shot down by anyone at any time.

glts mentioned this issue on Jun 9, 2021

CVE-2021-34555: Fix multi-value From rejection logic #178

Closed

cseres3 commented on Jun 10, 2021 — Author

I have now filed a CVE.

carnil commented on Jun 10, 2021

CVE-2021-34555 was assigned for this issue.

glts commented on Jun 14, 2021 — Contributor

It would be very helpful if those who saw crashing on their systems could try the patch and tell us if the problem is gone after or if there are other issues.

cseres3 commented on Jun 14, 2021 — Author

I can test it if you can send a ready-made RPM for CentOS8 or give step-by-step instructions for compiling it.

glts commented on Jun 14, 2021 — Contributor

I wouldn't know how to do that. Any other takers -- let us know if the patch helps.

Swallowtail23 commented on Jun 14, 2021

It's an easy compile and install on Centos 8. **@glts** Has it been merged into 'develop' stream yet?

Standard OpenDMARC on CentOS is EPEL package, and the 'develop' version can be compiled and run alongside it as it installs to /usr/local.

On my mail server (RHEL 8) I have both installed, and can switch between them. To do so, do this from a working directory somewhere:

```
git clone https://github.com/trusteddomainproject/OpenDMARC
cd OpenDMARC
git checkout develop
autoreconf -v -i
./configure --with-spf --with-spf2-include=/usr/include/spf2/ --with-spf2-lib=/usr/lib64/
make
make install
```

Copy /etc/opendmarc.conf to /etc/opendmarc-new.conf, and create a new systemd file at /usr/lib/systemd/system/opendmarc-new.service, with updates to PIDFile, EnvironmentFile and ExecStart:

```
PIDFile=/var/run/opendmarc/opendmarc-new.pid
EnvironmentFile=-/etc/sysconfig/opendmarc-new
ExecStart=/usr/local/sbin/opendmarc $OPTIONS
```

Create the environment file and edit to match.

In the config file at /etc/opendmarc-new.conf, use a different port for socket - I use

```
Socket inet:8894@localhost
```

...then make sure Postfix or whatever MTA you use is configured accordingly. E.g. in Postfix I have:

```
### Milter ports ###
# 8890 = spf-milter     (glts, new testing - https://gitlab.com/glts/spf-milter)
# 8891 = OpenDKIM
# 8892 = OpenARC        (beta)
# 8893 = OpenDMARC      EPEL stable (currently 1.4.1)
# 8894 = OpenDMARC-new  (1.4.1 develop from git)

# spf-milter, DKIM, ARC, DMARC (1.4.1 git):
smtpd_milters           = inet:127.0.0.1:8890,
                                inet:127.0.0.1:8891,
                                inet:127.0.0.1:8892,
                                inet:127.0.0.1:8894
```

Enable the new service

```
systemctl enable --now opendmarc-new
```

... and check.

Swallowtail23 commented on Jun 14, 2021

...noting that you will of course need the usual packages installed as required for compiling... and the sendmail-milter-devel package I believe is needed.

glts commented on Jun 15, 2021 — Contributor

Thanks **@Swallowtail23**. No, it's not in develop yet.

You can either use my fork instead:

```
git clone https://github.com/glts/OpenDMARC
cd OpenDMARC
git checkout fix-multi-value-from
```

Or apply the patch from the pull request, https://github.com/trusteddomainproject/OpenDMARC/pull/178.patch:

```
git clone https://github.com/trusteddomainproject/OpenDMARC
cd OpenDMARC
git checkout develop
patch -p1 < /path/to/178.patch
```

Swallowtail23 commented on Jun 15, 2021

> ./configure --with-spf --with-spf2-include=/usr/include/spf2/ --with-spf2-lib=/usr/lib64/

Please do note also that configure line I used is to use libspf2 not OpenDMARC's internal SPF code, alter as you need.

sriccio commented on Jun 15, 2021 • edited

Hello **@glts**

Thank you for the patch.

I've rebuilt the RPM (from the EPEL source RPM) adding the 178 patch + using tag rel-opendmarc-1-4-1-1 tar.gz
We were having 20-30 segfaults per day (I've used monit to monitor the process and restart it when it dies).
I'll report if the segfaults are still occuring with the patch.

Kind regards.

sriccio commented on Jun 15, 2021

@glts

No new segfaults since I'm using the patched version. Seems good. Thanks!

glts commented on Jun 16, 2021 Contributor

@sriccio Good to hear, thanks for testing

shawniverson commented on Jun 16, 2021

@sriccio do you have the SPEC file you would be willing to share for your rebuilt RPM? Just want to save a little time and get this out the door for others.

sriccio commented on Jun 16, 2021

@shawniverson

Here is attached the SRPM of the package I've rebuilt.

opendmarc-1.4.1.1-1.el7.src.zip

I hope it will be of help.

shawniverson commented on Jun 17, 2021

@sriccio thank you. I have packages build and in the repos for https://github.com/E-F-A/v4

apircalabu commented on Jul 11, 2021

Thanks for the fix and the SRPM. Be great if the binary version was updated too, it's still returning 1.4.1:
Jul 12 12:24:04 filter2 opendmarc[19086]: OpenDMARC Filter v1.4.1 starting (args: -c /etc/opendmarc.conf -P /run/opendmarc/opendmarc.pid)
strings /usr/sbin/opendmarc | egrep "1.4.."
1.4.1

quantumchaos451 commented on Jul 22, 2021

Given that there is a CVE against this issue, is there any particular reason it hasn't been merged into master yet?

Steve-Siirila commented on Jul 26, 2021

We were hit with this issue today as part of routine patching. We had to back out to previous version.

Does anyone have a concrete example I can use to trigger this problem? Simply specifying something like follows only causes a log message "multi-valued From field detected" but no crash:

From: UserA usera@domaina.com, UserB userb@domainb.com

I also tried leaving the domain part of of both to no avail, and actually got this error instead:

RFC 5322 requirement error: missing From field; accepting

glts commented on Jul 26, 2021 — Contributor

@Steve-Siirila When From: contains multiple recipients, an address with no domain part triggers the segfault. Use the patch further above.

Steve-Siirila commented on Jul 26, 2021

Thank you **@glts** -- I was able to duplicate with 1.4.1. I was literally leaving off just the domain parts, as in:

From: UserA usera@, UserB userb@

Once I removed the "@" characters it crashed as expected. Now we have a verification method after we upgrade to the latest version.

Swallowtail23 commented on Jul 27, 2021 • edited

EPEL repository have just pushed 1.4.1.1 for EL8
(EDIT)... but looking back through what is in it, I don't think it actually addresses this?

mricon commented on Jul 28, 2021

1.4.1.1 in EPEL contains the CVE fix:

```
* Sun Jul 11 2021 Kevin Fenzi <kevin@scrye.com> - 1.4.1.1-2
- Add patch for CVE-2021-34555. Fixes rhbz#1974707
```

👍 1

mskucherawy pushed a commit that referenced this issue on Dec 20, 2021

`Fix issue #179: Don't crash when a value in a multi-valued From field` ··· `80d18d3`

thegushi commented on Sep 8 — Collaborator

1.4.2 fixes this and has been released.

thegushi closed this as completed on Sep 8

thegushi self-assigned this on Sep 8

Assignees
thegushi

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

11 participants