

New issue

Jump to bottom

## CVE-2020-35766: Insecure temporary key path /tmp/testkeys #113

Open orlitzky opened this issue on Dec 28, 2020 · 10 comments

orlitzky commented on Dec 28, 2020

In <https://github.com/trusteddomainproject/OpenDKIM/blob/develop/libopendkim/tests/t-testdata.h#L15> a fixed path under `/tmp` is used for the test keys.

This is not a *huge* vulnerability, but it is a silly one since it is so well-known and easy to avoid: [https://owasp.org/www-community/vulnerabilities/Insecure\\_Temporary\\_File](https://owasp.org/www-community/vulnerabilities/Insecure_Temporary_File)

Either a random name should be chosen securely, or perhaps the temporary keys should be created within the build directory.

orlitzky mentioned this issue on Dec 28, 2020

**make -j <num> check failures #110**

Open

orlitzky changed the title ~~Insecure temporary key path /tmp/testkeys~~ CVE-2020-35766: Insecure temporary key path /tmp/testkeys on Dec 28, 2020

gits commented on Dec 29, 2020

Curious why this would be assigned a CVE. Tests are not part of the deployed software, so it's not possible to exploit this.

orlitzky commented on Dec 29, 2020 • edited

Author

It's exploitable whenever/wherever the test suite is run. If I `git clone` the repo and run the test suite, it's exploitable on my machine. In other words, the code is exploitable in 100% of the situations where it's used. And, for example, the test suite is optionally run whenever a Gentoo user installs OpenDKIM.

You're correct that you don't need to worry about this in a binary deb package, for example... but the guy building the deb needs to worry about it.

martinbogo commented on Dec 29, 2020

The CVE is "under investigation" -- and targets the test suite as was noted.

I'm on vacation till the 6th of January, and will hold off taking any action until the CVE is accepted/tested or resolved/rejected.  
...

orlitzky commented on Dec 29, 2020

Author

The CVE being issued doesn't mean much on its own... the number is just a way for everyone to refer to one vulnerability in a consistent way. (If you think the issue itself is invalid, it can be disputed.)

That the issue is exploitable is clear: create a symlink from `/tmp/testkeys` to `/etc/passwd` as any unprivileged user ( `nobody` , `www` , etc.). Then run the test suite as root. Now your system is borked.

martinbogo commented on Dec 29, 2020

Michael,

That requires something to be run "as root" which is unacceptable on `_any_` system by basic security measures. On that principle alone, the CVE is basically not valid. If an exploit requires you to run something `_as_` root for it to work in the first place, it's an error in procedure. Not an exploit.  
...

martinbogo commented on Dec 29, 2020

If you wish to repair the issue and submit a patch/PR, I'll look at it. Otherwise, this is a "doctor, it hurts when I do this" kind of bug ... don't run test suites as root.

On Tue, Dec 29, 2020 at 1:42 PM Martin Bogomolni <martinbogo@gmail.com> wrote:  
...

orlitzky commented on Dec 29, 2020

Author

If you wish to repair the issue and submit a patch/PR, I'll look at it. Otherwise, this is a "doctor, it hurts when I do this" kind of bug ... don't run test suites as root.

Replace "root" with the username of your choosing. Should random unprivileged accounts on the machine be able to delete his files?

mdomsch commented on Dec 29, 2020

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1911496](https://bugzilla.redhat.com/show_bug.cgi?id=1911496) (tracking bug)  
Affects: epel-all [bug 1911498] [https://bugzilla.redhat.com/show\\_bug.cgi?id=1911498](https://bugzilla.redhat.com/show_bug.cgi?id=1911498)  
Affects: fedora-all [bug 1911497] [https://bugzilla.redhat.com/show\\_bug.cgi?id=1911497](https://bugzilla.redhat.com/show_bug.cgi?id=1911497)

I'll hold off adjusting the packages in Fedora & EPEL until upstream has a recommended resolution.

orlitzky commented on Dec 29, 2020

Author

@mdomsch unless your users can run the test suite somehow, this probably doesn't affect your RPMs.

orlitzky commented on Dec 29, 2020

Author

@martinbogo there are a few ways to fix this, and some of them interact with #110.

If the test keys never change, one easy option would be to commit them to git, and avoid the race condition with building them entirely. You would probably want to keep the key-generating program around somewhere, though.

Another option would be to build they keyfile as part of the libopendkim build, outside of the "check" target, storing them in the build directory with the other libopendkim build stuff.

Finally, there's this option, mimicking the test-socket stuff that's already there, but doing nothing for #110:

```
diff --git a/configure.ac b/configure.ac
index 828fe53f..649338d6 100644
--- a/configure.ac
+++ b/configure.ac
@@ -2471,6 +2471,19 @@ then
     AC_SUBST(TESTSOCKET)
 fi

+
+#
+# specify test keyfile
+#
+AC_ARG_WITH([test-keys],
+    [AS_HELP_STRING([--with-test-keys],
+        [writable file path for temporary test keys]),
+    [testkeys="$withval"], [testkeys="./testkeys"])
+TEST_KEYS=$testkeys
+AC_DEFINE_UNQUOTED([TEST_KEYS],
+    ["${TEST_KEYS}",
+        [writable file path for temporary test keys]])
+
#
# Platform Specific Configuration
#
diff --git a/libopendkim/tests/t-testdata.h b/libopendkim/tests/t-testdata.h
index 1fd481c5..95dfcaf7 100644
--- a/libopendkim/tests/t-testdata.h
+++ b/libopendkim/tests/t-testdata.h
@@ -5,6 +5,7 @@
** Copyright (c) 2009-2012, The Trusted Domain Project. All rights reserved.
*/


+#include "build-config.h"

#define CRLF "\r\n"
#define SP " "
@@ -12,7 +13,7 @@
#define LARGEBOysize 65536
#define LARGELINESIZE 4100

-#define KEYFILE "/tmp/testkeys"
+#define KEYFILE TEST_KEYS


#define JOBID "testing"
#define SELECTOR "test"
```

I'm not 100% sure that `.` is always safe, but [https://www.gnu.org/software/autoconf/manual/autoconf-2.70/html\\_node/Preset-Output-Variables.html](https://www.gnu.org/software/autoconf/manual/autoconf-2.70/html_node/Preset-Output-Variables.html) says that `builddir` is rigorously defined to be `.`, and that's what I was aiming for, so...

 dotlambda mentioned this issue on Jan 28, 2021

Vulnerability roundup 98: opendkim-2.10.3: 1 advisory [7.8] NixOS/nixpkgs#109200

Closed

 1 task

Assignees

No one assigned

Labels

None yet

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

4 participants

