Copy Summary ▾ View ▾

Closed Bug 1692899 (CVE-2021-29948) Opened 2 years ago Closed 2 years ago

RNP-01-003 WP3 Thunderbird: Possible race condition when reading from disk

▾ **Categories**

Product:	MailNews Core ▾	Type:	defect
Component:	Security: OpenPGP ▾	Priority:	*Not set* Severity: --
Version:	78		

▾ **Tracking**

Status: RESOLVED FIXED
Milestone: 89 Branch

Tracking Flags:

	Tracking	Status
thunderbird_esr78	---	fixed
thunderbird88	---	fixed

▸ **People** (Reporter: KaiE, Assigned: KaiE)

▸ **References**

▸ **Details** (Keywords: sec-low)

▾ **Attachments**

Bug 1692899 - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin
2 years ago **Kai Engert (:KaiE:)**
48 bytes, text/x-phabricator-request

wsmwk : **approval-comm-beta+**
wsmwk : **approval-comm-esr78+**

Details | Review

Bottom ↓ Tags ▾ Timeline ▾

Kai Engert (:KaiE:) Assignee
Description • 2 years ago

When processing a PGP-signed email, the signature data is extracted and written to the filesystem before calling the RNP library, which in turn reads the signature data back from the filesystem. This introduces a race condition due to the timing and predictable file-path wherein a malicious local user can swap out the dumped file for a malicious signature file. During this assessment, however, it was not possible to exploit this in any meaningful way. The following shows a code excerpt that is responsible for writing the file to disk before calling the RNP library.

Affected File:
comm/mail/extensions/openpgp/content/modules/mimeVerify.jsm

Affected Code:

```
onStopRequest() {
[...]
if (this.protocol === PGPMIME_PROTO) {
[...]
this.sigFile = EnigmailFiles.getTempDirObj();
this.sigFile.append("data.sig");
this.sigFile.createUnique(this.sigFile.NORMAL_FILE_TYPE, 0x180);
EnigmailFiles.writeFileContents(this.sigFile, this.sigData, 0x180);
if (!EnigmailDecryption.isReady(win)) {
return;
}
let sigFileName = EnigmailFiles.getEscapedFilename(
EnigmailFiles.getFilePath(this.sigFile)
);
let keyserver = EnigmailPrefs.getPref("autoKeyRetrieve");
let options = {
keyserver,
keyserverProxy: EnigmailHttpProxy.getHttpProxy(keyserver),
fromAddr: EnigmailDecryption.getFromAddr(win),
mimeSignatureFile: sigFileName,
};
const cApi = EnigmailCryptoAPI();
[...]
this.returnStatus = cApi.sync(cApi.verifyMime(this.signedData, options));
[...]
```

It is recommended to avoid using the filesystem in order to pass the signature information to the library. Instead, the information should be passed via memory, as done with the signed data itself.

Kai Engert (:KaiE:) Assignee
Comment 1 • 2 years ago

Attached file ***Bug 1692899 - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin*** *— Details*

Phabricator Automation
Updated • 2 years ago

Assignee: nobody → kaie
Status: NEW → ASSIGNED

Kai Engert (:KaiE:) Assignee
Comment 2 • 2 years ago

https://hg.mozilla.org/comm-central/rev/83e6e80e5adfddf3d6e1af6fa15283a966df5e60

Status: ASSIGNED → RESOLVED
Closed: 2 years ago

Resolution: --- → FIXED
Target Milestone: --- → 89 Branch

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

status-thunderbird89: --- → affected
status-thunderbird_esr78: --- → affected

Kai Engert (:KaiE:) Assignee
Comment 3 • 2 years ago

Comment on attachment 9211305 [details]
~~Bug 1692899~~ - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin

[Approval Request Comment]
Regression caused by (bug #): no
User impact if declined: none
Testing completed (on c-c, etc.): c-c
Risk to taking this patch (and alternatives if risky): low

Attachment #9211305 - Flags: approval-comm-beta?

Wayne Mery (:wsmwk)
Comment 4 • 2 years ago

Comment on attachment 9211305 [details]
~~Bug 1692899~~ - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin

[Triage Comment]
Approved for beta

Attachment #9211305 - Flags: approval-comm-beta? → approval-comm-beta+

Kai Engert (:KaiE:) Assignee
Comment 5 • 2 years ago

https://hg.mozilla.org/releases/comm-beta/rev/bdbc5d1155e8336f65f46182cd25f6b07013f6e3
88.0b2

status-thunderbird88: --- → fixed

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

status-thunderbird89: affected → ---

Kai Engert (:KaiE:) Assignee
Comment 6 • 2 years ago

Comment on attachment 9211305 [details]
~~Bug 1692899~~ - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin

approval info: see ~~comment 3~~.

We can wait for 78.10

Attachment #9211305 - Flags: approval-comm-esr78?

Wayne Mery (:wsmwk)
Comment 7 • 2 years ago

Comment on attachment 9211305 [details]
~~Bug 1692899~~ - Don't use a file for passing OpenPGP signature data between modules. r=mkmelin

[Triage Comment]
Approved for esr78

Attachment #9211305 - Flags: approval-comm-esr78? → approval-comm-esr78+

Kai Engert (:KaiE:) Assignee
Comment 8 • 2 years ago

https://hg.mozilla.org/releases/comm-esr78/rev/283e7c77ae9dea08ca9ec2c7ab448b8a3d08ac1a
78.10

status-thunderbird_esr78: affected → fixed

Frederik Braun [:freddy]
Updated • 2 years ago

Alias: CVE-2021-29948

Frederik Braun [:freddy]
Comment 9 • 2 years ago

I'm drafting security advisories for Thunderbird and need a security rating.
Given this requires a local user *and* has not been verified as exploitable, I will go with sec-low.
Let me know if you disagree and I'll happily adjust the advisory :)

Keywords: sec-low

Kai Engert (:KaiE:) Assignee
Comment 10 • 2 years ago

Thanks Freddy, rating and advisory text sounds good to me!

Wayne Mery (:wsmwk)
Updated • 2 years ago

−

Group: ~~mail-core-security~~

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

Top ↑