SOURCEFORGE

Home / Browse / Enigmail / Bugs

Enigmail Bugs

OpenPGP addon for Mozilla Thunderbird

Brought to you by: pbrunschwig

#721 Efail: Full Plaintext Recovery in PGP via Chosen-Ciphertext Attack

Status: fixed	**Owner:** nobody	**Labels:** None	
Found in Version: 1.9.8	**Severity:** Major	**Thunderbird version:** all	**GnuPG version:** all
Fixed in version: 2.0	**Cc:** nobody		**Operating System:** All
Updated: 2018-05-15	**Created:** 2017-11-23	**Creator:** Sebastian Schinzel	**Private:** No

Pretty Good Privacy (PGP) is an encryption scheme for email content, providing end-to-end confidentiality, integrity and authenticity. We describe a critical attack that leads to a full plain- text recovery. For the attack, the attacker needs to get read access (passive) to a PGP encrypted email, from which he knows the plaintext of some ten successive bytes. For uncompressed email plaintexts, this assumption usually holds. For deflate compressed plaintexts (the default for most messages) it gets more complicated as knowledge of parts of the plaintext is not sufficient. The attacker needs to know bytes of the compressed plaintext, which change even with small changes in the plaintext.
Given that the attacker knows the plaintext of one complete block (assuming blocksize 16 bytes), he then modifies the ciphertext in a specific way and sends it to the victim. The victim needs to view the message in order to trigger the plaintext leak. The attack requires no other action from the victim and we expect the attack to work with default configuration settings for most mail clients.

For details, please see the attached PDF.

1 Attachments

pgp_disclosure_thunderbird-20171123.pdf

Discussion

Patrick Brunschwig - *2017-11-24*

See also https://bugzilla.mozilla.org/show_bug.cgi?id=1420217 (which refers to the same issue).

Patrick Brunschwig - *2017-11-25*

I tried to use 01-dec-pgp-smime-html-reply.eml to see the effect of replying to a html/iframe message (section 7.1.1 of the document). I replaced the encrypted message with something I can decrypt. However, using Thunderbird 57.0b2 the result doesn't contain any of the decrypted message part.

Do I need to consider something specific?

Sebastian Schinzel - *2017-11-25*

Could you please add Jens Müller (jens.a.mueller@rub.de) to this bug. He is the original author of this finding.

Patrick Brunschwig - *2017-11-25*

I would need to know Jens' Sourceforge account name

Patrick Brunschwig - *2017-11-25*

Never mind, I think my test message wasn't well formatted. I can reproduce the error now.

Sebastian Schinzel - *2017-12-04*

Can we talk about how and when we disclose these bugs? What is the current state for patches/mitigations? Should we have a call to start discussions?

Patrick Brunschwig - *2017-12-05*

As far as I can tell, the only fixes I can do in Enigmail concern sections 7.1.1 and 7.1.2 of the document, and only for PGP/MIME messages. I cannot alter default behavior of Thunderbird that goes down to the HTML engine. And the only thing I can do for sections 7.1.1/7.1.2 is to warn the user - again I cannot change the default TB behavior.

As it happens there was recently a security audit that revealed a similar issue, such that the change for your case was only a more specific information message.

I'm planning to release these changes in about a week together with those other vulnerability issues.

If you test the latest nightly builds of Enigmail, you can see how Enigmail warns the user.
http://www.enigmail.net/index.php/en/download/nightly-build

Sebastian Schinzel - *2017-12-06*

Patrick, can we please coordinate the amount of information that you make public for the patches? We are not yet ready for public disclosure of the different bugs. In parallel, we are talking to gnupg and Thunderbird as well as several others. You were among the very first that we disclosed the issues to and we would appreciate if we can coordinate this with the other vendors. Ok?

Patrick Brunschwig - *2017-12-06*

Sure. I propose that I won't mention anything until you tell me to do so. The reason is that the warning message was introduced independently of this bug, while fixing other issues. Those issues will be mentiontioned, but they don't look in any way like what you found.

Would that be OK with you?

Sebastian Schinzel - *2017-12-06*

Sounds great. Thanks Patrick!

Patrick Brunschwig - *2018-02-11*

Is there any update to this?

Sebastian Schinzel - *2018-02-11*

Current plan is for coordinated disclosure at 17th of April. Attached the redacted paper submitted to USENIX Security. Please treat this confidential!

efail-usenix18-Thunderbird.pdf

Sebastian Schinzel - *2018-02-13*

Hey Patrick, should we schedule a phone call?

Patrick Brunschwig - *2018-02-13*

Sure we can. I suggest we coordinate this outside of this bug. I'll send you a direct mail.

Patrick Brunschwig - *2018-02-13*

I just fixed the MDC issue on Enigmail, if gpg signals "decryption failed", Enigmail doesn't return any data to the user anymore.

That's implemented on master and backported on the 2.0-branch.

Patrick Brunschwig - *2018-05-14*

- **status**: open --> fixed
- **private**: Yes --> No
- **Fixed in version**: --- --> 2.0

Patrick Brunschwig - *2018-05-14*

Now that the press release is out, I removed the "private" flag and publish the information.

I find it **very** disappointing that the EFF suggests to remove Enigmail (and some other tools).

Aritam - *2018-05-15*

It is indeed a bit confusing to general users that this bug is marked as fixed here and yet an ecosystem involving Thunderbird and Enigmail at their latest versions could still present vulnerabilities related to this issue. Given the publicity surrounding this disclosure, perhaps a dedicated attention-grabbing message on the main Enigmail website addressing this matter would be a good idea?