A Unified Timeline

flaked.sockpuppet.org/2018/05/16/a-unified-timeline.html

Thomas H. Ptacek

16 May 2018

A unified timeline of Efail PGP disclosure events

This is an attempt to combine public sources regarding when various PGP vendors were notified about Efail.

Sources:

- Efail: the Münster/Ruhr research team's public Efail.de site.
- #721: Enigmail bug #721
- Koch: Werner Koch's 5/14/2018 GnuPG mailing list post
- Hansen: Robert J. Hansen's Twitter feed.

10/25/17 (Efail)

~200 days before the embargo on the research breaks, the Efail team contacts the Mozilla Thunderbird team, opening bug #1411592 (this bug is still private today).

11/3/17 (Efail)

The Efail team contacts Google, presumably regarding the S/MIME variant of their attack.

11/23/17 (#721)

The Efail team opens bug #721, "Efail: Full Plaintext Recovery in PGP via Chosen-Ciphertext Attack". This bug log is now public. The initial report includes an early draft of the Efail paper, and refers back to (private) Thunderbird bug #1420217.

11/24/17 (Koch)

According to Werner Koch from GnuPG, the Efail team sends an "advisory" (probably a version of the paper sent to Enigmail) to GnuPG. Koch replies that the PGP MDC prevents the Efail attack. Efail points out that they can roll back MDC PGP messages to non-MDC messages.

11/25/17 (#721)

Patrick Brunschwig from Enigmail discusses the Efail bug with Sebastian Schinzel from Efail (Brunschwig and Schinzel are the only representatives of their projects to converse so from now on I'll refer to them as "Enigmail" and "Efail").

11/26/17 (Koch)

Koch responds that GnuPG prints an error (starting in October of 2015) when the MDC is stripped from messages, and Enigmail is “doing something wrong”.

11/29/17 (Koch)

Efail asks Koch for a phone call; Koch never replies.

12/04/17 (#721)

Efail asks Enigmail about a timeline for disclosure.

12/05/17 (#721)

Enigmail tells Efail a release with fixes will be available “in about a week”, with a nightly build available immediately.

12/06/17 (#721)

Efail reminds Enigmail that they’re coordinating with other vendors and asks that details not be included in the patch; Enigmail agrees.

2/10/18 (Efail)

Multiple vendors, including Thunderbird and Apple Mail, are notified of the Efail “direct exfiltration” attack, which uses MIME directly to inject HTML rather than tampering with cipher text.

2/11/18 (#721)

Enigmail asks Efail for a disclosure date; Efail responds with the proposed announcement date (in April) and a preprint of their Usenix paper. The 2/11 preprint is fairly close to the final Usenix version, but is redacted so that only information pertinent to Enigmail is identifiable.

2/13/18 (#721)

Efail requests phone call with Enigmail, who agrees. Coordination happens off the bug tracker. Enigmail reports back new fixes, and says they’re backported.

2/15/18

90 days back from the ultimate disclosure date, this would be the start of the Google Project Zero mandatory disclosure window.

2/16/18 (Efail)

GPGTools is notified of the PGP-based (presumably: non-direct-exfiltration) variants of the Efail attack.

4/17/18

Proposed public announcement date as relayed to Enigmail in #721.

4/27/18 (Koch)

Werner Koch obtains a copy of the KMail preprint of the Efail paper. Koch discusses with some members of the GnuPG team. No further action is taken “[…] because due to the redaction we were not able to contact and help the developers of other MUAs which might be affected.”

5/11/18 (Hansen)

Robert Hansen of the GnuPG and Enigmail projects is notified by either Enigmail or GnuPG about Efail, and somehow receives the KMail version of the Efail paper.

5/14/18 (Hansen)

Efail is publicly announced. Robert J. Hansen “takes point” for handling of disclosure for one or both of Enigmail and GnuPG, claims not to have been given any information about Efail prior to the “samizdat” copy of the paper he obtained on 5/11/18 — presumably sometime after he failed to obtain it from a journalist, who, Hansen, says, indicated to him that the paper had been embargoed only to journalists and away from researchers. Hansen is affiliated with both GnuPG and Enigmail and is listed as a project team member for Enigmail, which received an almost complete preprint of the paper in February.

Koch

#721

Efail