Efail press release

Robert J. Hansen rjh at sixdemonbag.org
Mon May 14 14:27:44 CEST 2018

- Previous message (by thread): Mailpile on Efail
- Next message (by thread): US-CERT now issuing a warning for OpenPGP-SMIME-Mail-Client-Vulnerabilities
- **Messages sorted by:** [date] [thread] [subject] [author]

Over the last few hours, Werner, Andre, and I have been working on an
official statement about the Efail paper. Without further ado, here it is.

An Official Statement on New Claimed Vulnerabilities
== ======== ========= == === ======= ===============
by the GnuPG and Gpg4Win teams

(This statement is only about the susceptibility of OpenPGP, GnuPG, and
Gpg4Win. It does not cover S/MIME.)

Recently some security researchers published a paper named "Efail:
Breaking S/MIME and OpenPGP Encryption using Exfiltration Channels".
The EFF has gone so far as to recommend immediately uninstalling
Enigmail. We have three things to say, and then we're going to show you
why we're right.

1. This paper is misnamed.

2. This attack targets buggy email clients.

3. The authors made a list of buggy email clients.

In 1999 we realized OpenPGP's symmetric cipher mode (a variant of cipher
feedback) had a weakness: in some cases an attacker could modify text.
As Werner Koch, the founder of GnuPG, put it: "[Phil Zimmermann] and Jon
Callas asked me to attend the AES conference in Rome to discuss problems
with the CFB mode which were on the horizon. That discussion was in
March 1999 and PGP and GnuPG implemented a first version [of our
countermeasure] about a month later. According to GnuPG's NEWS file,
[our countermeasure] went live in Summer 2000."

The countermeasure Werner mentions is called a Modification Detection
Code, or MDC. It's been a standard part of GnuPG for almost eighteen
years. For almost all that time, any message which does not have an MDC
attached has caused GnuPG to throw up big, clear, and obvious warning
messages. They look something like this:

```
    gpg: encrypted with 256-bit ECDH key, ID 7F3B7ED4319BCCA8, created
2017-01-01
          "Werner Koch <wk at gnupg.org>"
    [GNUPG:] BEGIN_DECRYPTION
    [GNUPG:] DECRYPTION_INFO 0 7
    [GNUPG:] PLAINTEXT 62 1526109594
    [GNUPG:] PLAINTEXT_LENGTH 69
    There is more to life than increasing its speed.
                    -- Mahatma Gandhi
    gpg: WARNING: message was not integrity protected
    [GNUPG:] DECRYPTION_FAILED
    [GNUPG:] END_DECRYPTION
```

GnuPG also throws large warning messages if an MDC indicates a message
has been modified. In both cases, if your email client respects this
warning and does the right thing -- namely, not showing you the email --
then you are completely protected from the Efail attack, as it's just a
modern spin on something we started defending against almost twenty
years ago.

If you're worried about the Efail attack, upgrade to the latest version
of GnuPG and check with your email plugin vendor to see if they handle
MDC errors correctly. Most do.

You might be vulnerable if you're running an ancient version of GnuPG
(the 1.0 series; the current is 2.2), or if your email plugin doesn't
handle GnuPG's warning correctly. You might also have had some exposure
in the past if back then you used a pre-2000 version of GnuPG, and/or an
email plugin which didn't handle the warning correctly.

We made three statements about the Efail attack at the beginning. We're

```
going to repeat them here and give a little explanation.  Now that we've
explained the situation, we're confident you'll concur in our judgment.

1.  This paper is misnamed.  It's not an attack on OpenPGP.  It's an
attack on broken email clients that ignore GnuPG's warnings and do silly
things after being warned.

2.  This attack targets buggy email clients.  Correct use of the MDC
completely prevents this attack.  GnuPG has had MDC support since the
summer of 2000.

3.  The authors made a list of buggy email clients.  It's worth looking
over their list of email clients (found at the very end) to see if yours
is vulnerable.  But be careful, because it may not be accurate -- for
example, Mailpile says they're not vulnerable, but the paper indicates
Mailpile has some susceptibility.

The authors have done the community a good service by cataloguing buggy
email email clients.  We're grateful to them for that.  We do wish,
though, this thing had been handled with a little less hype.  A whole
lot of people got scared, and over very little.
```

- Previous message (by thread): Mailpile on Efail
- Next message (by thread): US-CERT now issuing a warning for OpenPGP-SMIME-Mail-Client-Vulnerabilities
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Gnupg-users mailing list