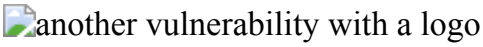
HackDefense IT Security Testing Advice



#EFail - the security industry and the importance of nuance

by Mark Koek on 14-May-2018

Today, details were rushed out regarding two serious vulnerabilities that might enable a determined attacker to decrypt users' encrypted e-mails. Not just current ones, but older e-mails too. Doesn't that sound alarming?

Unfortunately, the people who discovered the vulnerabilities and collectively labeled them #EFail didn't think this sounded alarming enough, and started a disclosure process that went off the rails, resulting in some seriously bad advice to people dealing with very sensitive information.

The issues

In summary, both issues allow an attacker to embed content encrypted to your private key inside an URL in an <img> tag in an HTML-formatted e-mail. The e-mail client then:

1. decrypts that content using your private key, and
2. fetches the image using the URL (which now contains decrypted data, thus revealing the plaintext to the owner of the website the image is fetched from, presumably controlled by the attacker).

This, apparently, works against many e-mail clients, using PGP/MIME and/or S/MIME.

Good reason to immediately patch your e-mail client and to re-check that you disabled "remote content loading" (default in many clients including Mozilla Thunderbird) or even that you have disabled HTML e-mail entirely.

The response

What is *not* a good idea (to put it very mildly) is to stop encryption of your e-mail altogether. Yet this is precisely what a severely misguided warning prior to the release of the details ended up recommending. Predictably, this was exaggerated some more by some news media (UNINSTALL NOW!).

We can only hope that nobody got in trouble because somebody could freely snoop on their e-mail today. As we know from past experience some governments are extremely interested in the contents of their citizens' e-mail. They will be happy to learn about #efail, but even happier if some of their subjects followed the advice to switch off encryption today.

Phased disclosure

Another puzzling aspect of the disclosure process in this case is that a warning was sent out containing what I humbly consider bad advice, without actually telling us the details. They were scheduled to be released early tomorrow morning (for us in Europe at least, for those unfortunate enough to live in the Americas it would have been the middle of the night). After an outcry, authors of the software maligned as being less-secure-than-plaintext broke the embargo and started to reveal details. After that the authors released the full paper ahead of schedule.

We can only speculate why they thought the delayed disclosure was a good idea (I have asked, but not received any reply yet). Presumably patches were to appear tomorrow morning in sync with the announcement, and we would all be put on alert to install them immediately.

I'll try to post more about that tomorrow as this story develops... Update 2018-05-16 - *No update. Either e-mail software was already patched, or declared not really vulnerable at all. What remains a mystery is why the researchers have waited 6 months to disclose (they first approached software authors about these issues in secret in November 2017), but then when the big day of disclosure comes, what, if any, remediation is available is still unclear.*

Lessons for the industry

Almost immediately, there was pushback from the security community against the alarmist announcement that was initially sent out. People behind the extremely valuable e-mail project Enigmail, for example, started politely disagreeing with EFail's discoverers. Considering that they had already patched their software, and that the EFail people were still promoting that users should disable it, they may have realised they were being a bit too polite. Shortly afterwards, the researches grudgingly published details on efail.de because the embargo was broken.

The understandable pushback then caused less technical users to conclude this was all a hoax and that there was nothing they needed to do. Which is, of course, a big mistake - there is definitely a serious security vulnerability here and updates need to be made available and installed as soon as possible.

So what could have been done differently?

- We need to stop giving vulnerabilities names, logos, and domain names. Really. There is a good, working numbering scheme to reference vulnerabilities. Vanity does not help getting taken seriously.
- Include mitigating factors in your communications. For example, efail.de makes no mention of the fact that major software products affected by the bugs are not vulnerable in their default configuration. This, again, will cause you - rightly or wrongly - to be suspected of over-hyping.
- Make sure patches are available before you release the information, so you can give users the best possible advice. "Stop using encryption" because you have found a weakness in an

encryption scheme is not acceptable. There are organisations such as the CERT Coordination Center that can help you with co-ordinated disclosure for free.

It's 2018 and finally, IT security is getting some much-needed attention from non-technical people. But we are (still) trying to get attention by over-emphasizing vulnerabilities and under-emphasizing mitigating factors. As a result, the media (already prone to over-hyping) are going into overdrive.

We need to realise that this media overdrive will soon turn against us if we keep exaggerating the risk. Just give correct, nuanced and well-researched information and make sure users can then help themselves based on their own particular situation.

Feedback welcome!

IT Security | Testing | Advice

HackDefense

1. Security & Privacy Compliance
2. Contact