No, PGP is not broken, not even with the Efail vulnerabilities (protonmail.com)

203 points by dsr12 12 months ago | hide | past | web | favorite | 27 comments

georgyo 12 months ago [-]

Finally, a company not using this attack as a way to say PGP is fully broken and you should be using their walled garden instead of PGP.

I don't even understand why efail is getting so much publicity. The attack requires privileges access to your computer or your mail server in order to modify your existing messages. Or the ability to intercept messages in flight. That is a huge barrier, and if they had that access, all your plain text email is compromised as well.

I don't understand why people are uninstalling gnupg because of this "attack". I am extremely upset at the email keybase sent me, basically telling me that to be secure I should unregistered my PGP key; complete with instructions on how to do so. Accourding to them, I should be only using keybase's home grown encryption tools.

This whole exploit just seems like a marketing attack.

> icebraining 12 months ago [-]
>
> Isn't securing messages in flight the point of PGP?
>
> *if they had that access, all your plain text email is compromised as well.*
>
> Isn't that why we're using PGP in the first place? If plain text email can be assumed to not be compromised, why encrypt at all?
>
> > tinus_hn 12 months ago [-]
> >
> > There is a difference between making sure what you get is what was sent by the sender and making sure no one but you and the sender can read the message.
> >
> > Compromising mail using this vulnerability requires manipulating it while it is being sent which is more difficult than just tapping the connection.

kakwa_ 12 months ago [-]

> The attack requires privileges access to your computer or your mail server in order to modify your existing messages

True, if your computer is hacked, you are fd (as always may I add).

But, the point of PGP and S/MIME is to provide end-to-end encryption, i. e. from the sender to the recipient. You don't trust the MTAs and MDA in between, their only role is to transmit the email.

So this flaw is kind of critical. However, it's far from being the end of the world, this flaw is somewhat visible, if it was exploited massively in the wild, it would have been known by now.

As a side note, S/MIME or PGP email is quite horrible as a standard, first the title is not encrypted by default, and being able to mix encrypted and not encrypted data in the body is really weird.

I don't understand how something like that could have been considered good. There are probably 1 or 2 gotchas, but having an all or nothing encryption seems preferable, the whole message apart from a few headers used for delivery (sender, recipient, DKIM, etc) should be completely encrypted or not. Also, if remote content was forbidden for encrypted messages, this would be a good thing.

> ianstormtaylor 12 months ago [-]
>
> Your own comment equates the level of protection PGP provides to that of plaintext. Which sounds to me like another way of saying, “PGP is broken”.
>
> > Bartweiss 12 months ago [-]
> >
> > I agree that this is the wording of the comment - if having a PGP-encrypted message intercepted in transit compromises it, something has gone horribly wrong.
> >
> > Fortunately, it's not true; the situation is actually much better than the comment suggests. As the Protonmail rundown points out, the better PGP clients should be unaffected, and secure even with in-transit interception.
> >
> > > mtremsal 12 months ago [-]
> > >
> > > Unless another recipient uses a flawed client, which is pretty hard to check.
> > >
> > > > Bartweiss 12 months ago [-]
> > > >
> > > > If securing the contents of the message are the issue, then this is true but it's an opsec problem - no different than corresponding with someone who's downloaded malware.
> > > >
> > > > But "another recipient leaked the data" isn't actually the same security breach as "my data was observed". If the message was sent twice to different people, no

one even has reason to believe I was sent the data. If the message was sent with multiple recipients, GPG encrypts it symmetrically, then provides an encrypted copy of that key to each user - which means there's no way to check that I actually received a valid copy of the message.

It's a good point, though, that if you're planning the Arab Spring by group email or something, you should currently treat messages as at higher risk even if you use Protonmail.

nzp 12 months ago [-]

Another recipient could also work for cops, which is also pretty hard to check.

bonzini 12 months ago [-]

> Your own comment equates the level of protection PGP provides to that of plaintext

Not really. PGP provides both signing and encryption. Encrypted *unsigned HTML* messages have the same level of protection as plaintext, but that adds two very strong qualifiers. Encrypted unsigned messages already make little sense and should be a red flag.

bdhess 12 months ago [-]

> Encrypted unsigned messages already make little sense and should be a red flag.

Confidentiality is a separate concern from authenticity of the source. There are obvious cases where the authenticity of the source is irrelevant, e.g. if a message contains anonymous feedback or a tip.

leetcrew 12 months ago [-]

> Finally, a company not using this attack as a way to say PGP is fully broken and you should be using their walled garden instead of PGP.

i mean, i do like protonmail and their product, but you can't act like this post isn't designed to protect their own interests. the facts happen to be on their side here.

AdmiralAsshat 12 months ago [-]

> I don't even understand why efail is getting so much publicity.

Because many people have a defeatist, preconceived notion that the government can monitor anything and everything you do, no matter what you do. A flaw in PGP is a key piece of evidence in support of their theory that allows them to say, "See? All those tinfoil hats spent all that time on a cumbersome solution that was defeated anyway."

Xylakant 12 months ago [-]

a lot of the criticism that GPG receives can be summarized as "GPG has known to be problematic for at least a decade, move on to something better". And, given the nature of the underlying issue - allowing access to unauthenticated plaintext by default - this is valid. The fix has been known for at least 10 years - add a checksum/authenticator. I can understand accepting messages that don't have message authentication for a handful of years for BC reasons, but at some point, GPG should have switched: Don't present plaintext at all if you can't authenticate it. You can still allow access to unauthenticated plaintext, but make that an explicit option. That alone would have prevented this issue and that's really on GPGs side.

baby 12 months ago [-]

> The attack requires privileges access to your computer or your mail server in order to modify your existing messages

So you're saying that PGP is useless?

diamondo25 12 months ago [-]

No he is saying it requires a man-in-the-middle kind of attack. Additionally, it requires a broken mail client that does not check error result from the pgp decoder _and_ concatenates different mail parts _and_ has HTML rendering enabled (and does not warn for external content). The pgp spec, afaik, had already protection by checking inline modification (fixing the exploit using CBC), but due to old mail clients this didnt generate an error by default. Some users of the gpg decoder tool does not support or ignore errors, making you invisible from issues in the email... Check the efail.de page for more info.

baby 12 months ago [-]

> it requires a man-in-the-middle kind of attack

Yeah that's exactly what PGP is supposed to protect against.

VyseofArcadia 12 months ago [-]

I can't wait to discover that the whole thing was engineered by or at least sponsored by a nefarious three letter agency.

Clubber 12 months ago [-]

Yes, "PGP has a flaw so you should disable plugins," sounds extremely fishy.

Xylakant 12 months ago [-]

AFAIR the attack allows taking any old encrypted email and modifying it in a fashion so that a vulnerable client at the recipient would decrypt the message and send its content to the attacker. So the attacker needs access to the mail, either from the victims computer, mail-server or any or the senders computer, mail server (sent mail imap box) or intercepted in flight and the ability to send that to the recipient. It's not like this is necessarily hard, this is what GPG is supposed to protect against.

disabling the plugin until this is fixed would prevent an attack. Depending on your risk profile, this would be a reasonable mitigation: Don't receive encrypted messages for a while, but keep old conversations safe.

Analemma_ 12 months ago [-]

If one or two clients don't implement the standard correctly, the clients are broken. If *all but* one or two clients don't implement the standard correctly, the standard is broken. Part of what makes good standard design is knowing how to avoid pitfalls in client implementation.

zokier 12 months ago [-]

Most clients do not implement (correctly or incorrectly) PGP at all. Instead they delegate the PGP parts to GnuPG, and failed to handle the warnings that GPG emitted. So your logic could be applied to GPG and argued that it is broken.

TooBrokeToBeg 12 months ago [-]

> So your logic could be applied to GPG and argued that it is broken.

That's a pretty common claim and has been for a long time. It's not just verification of identity, but verification of integrity that the encryption is supposed to enforce. Instead, it throws a warning for one case and will not decrypt for another. The binary client is broken, as a security tool (insofar as it fails to provide the security it claims). If the integrity of the message is compromised, why show a version of the decrypted message at all? There's no guarantee that's correct and has led to this.

Forge36 12 months ago [-]

If true in curious how error handling is being done. Throwing an exception if possible might cause this case to crash the program. Or not returning the decoded content on exception and printing an error message in place of the content

StreamBright 12 months ago [-]

Well there is more to it though:

https://secushare.org/PGP

https://www.ctrlc.hu/~stef/blog/posts/on_pgp.html

dvdgsng 12 months ago [-]

That first link is just a list of known short comings of PGP (wrong usage, infrastructure, metadata, etc), but none of them is a reason to not use PGP at all. PGP might not be encryption for the masses, but at least encryption that works.

beders 12 months ago [-]

MIME parsers are broken. End of story.