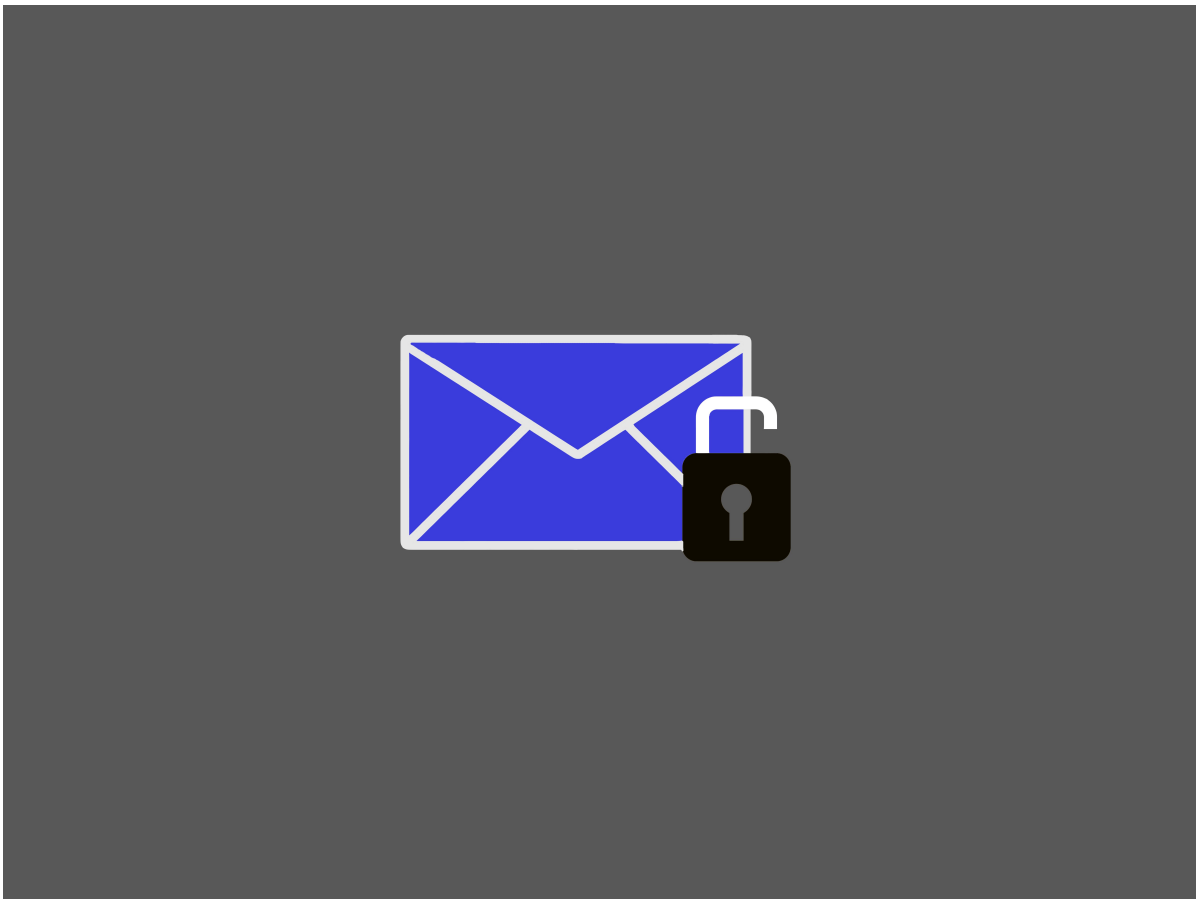
Encrypted Email Has a Major, Divisive Flaw

wired.com/story/efail-encrypted-email-flaw-pgp-smime

Lily Hay Newman



An attack called eFail overcomes the protections of encrypted email standards PGP and S/MIME.

Getty Images

The ubiquitous email encryption schemes PGP and S/MIME are vulnerable to attack, according to a group of German and Belgian researchers who posted their findings on Monday. The weakness could allow a hacker to expose plaintext versions of encrypted messages—a nightmare scenario for users who rely on encrypted email to protect their privacy, security, and safety.

The weakness, dubbed eFail, emerges when an attacker who has already managed to intercept your encrypted emails manipulates how the message will process its HTML elements, like images and multimedia styling. When the recipient gets the altered message and their email client—like Outlook or Apple Mail—decrypts it, the email program will also load the external multimedia components through the maliciously altered channel, allowing the attacker to grab the plaintext of the message.

You've Got eFail

The eFail attack requires hackers to have a high level of access in the first place that, in itself, is difficult to achieve. They need to already be able to intercept encrypted messages, before they begin waylaying messages to alter them. PGP is a classic end-to-end encryption scheme that has been a go-to for secure consumer email since the late 1990s because of the free, open-source standard known as OpenPGP. But the whole point of doing the extra work to keep data encrypted from the time it leaves the sender to the time it displays for the receiver is to reduce the risk of access attacks—even if someone can tap into your encrypted messages, the data will still be unreadable. eFail is an example of these secondary protections failing.

Sebastian Schinzel, one of the researchers on the project who runs the IT security lab at the Münster University of Applied Sciences, tweeted early Monday morning that, "There are currently no reliable fixes for the vulnerability. If you use PGP/GPG or S/MIME for very sensitive communication, you should disable it in your email client for now." The Electronic Frontier Foundation issued a similar warning, that "users should arrange for the use of alternative end-to-end secure channels, such as Signal, and temporarily stop sending and especially reading PGP-encrypted email," until there are patches or other mitigations for vulnerable email clients.

This advice has seemed overly reactionary to some cryptographers, though, who argue that some people can't simply switch to other secure platforms and that encrypted email is still better than nothing. The bigger issue, they argue, is the lack of unity in securing email in the first place and dealing with problems as they arise.

> 'The core architecture of PGP encryption is very dated.'

Kenn White, Open Crypto Audit Project

"For people who must use encrypted mail, there's not consensus yet on the best course of action," says Kenn White, director of the Open Crypto Audit Project. "Many people have criticized the EFF guidance, which is basically to stop using encrypted mail. I'm not sure such advice is warranted, or even practical." One option for now is to patch your encrypted email plugins whenever those updates come through, and disable as much remote image and custom HTML execution as possible.

Essentially, you want to set your PGP plugin to only show you the text of a message and not any of the fancy formatting or other media the sender included. The eFail researchers did find, though, that many email clients are overly lax in interacting with remote servers, meaning that even when you add restrictions you may not be able to completely control these interactions with potentially sketchy servers.

Ignored Warnings

Researchers have known about the theoretical underpinnings of the eFail attack since the early 2000s, and some implementations of the OpenPGP standard already protect against it. Since the attack centers around manipulating custom HTML, systems can and should be able to flag that the email the target actually receives has been altered. The message authentication check for PGP is called "Modification Detection Code," and MDCs indicate

the integrity of a message's authentication. But eFail highlights that many email clients will tolerate messages with invalid or missing MDCs instead of dropping them to ease friction between different PGP implementations.

In a statement, Werner Koch—the developer behind the popular, free PGP implementation GNUPrivacyGuard—noted that it took awhile for MDC adoption to pick up among PGP services. As a result, GNUPrivacyGuard and others worried that there would be too much service disruption for users if a missing MDC instantly resulted in a message being dropped. So instead of generating a full-on error, GNUPrivacyGuard and other implementations issue a warning—one that many email clients choose to simply ignore.

"The core architecture of PGP encryption is very dated, and in order to make current email apps able to still receive encrypted mail sent from older programs or read messages using older-style encryption, many software packages tolerate insecure settings," White says. "When a message is unable to be properly decrypted, instead of displaying a corruption error message—a 'hard fail' as it's known—the mail software will display the message anyway. Combined with other default conveniences like displaying images or loading links sent by the sender by default, the game is up."

> 'People don’t pay attention unless there’s an attack.'
>
> Matthew Green, Johns Hopkins University

At least MDC gives PGP some potential protection. The S/MIME standard—often used in corporate email encryption—currently has none. In tests of 35 S/MIME email clients, the researchers found that 25 had plaintext exfiltration weaknesses. Of 28 OpenPGP clients they tested, 10 were vulnerable. Though some of the details of the disclosure are still unclear, and Münster University of Applied Sciences's Schinzel has not yet returned a request from WIRED for comment, it seems that the researchers have been notifying impacted email client developers since at least fall 2017. Hopefully this means that patches are on their way.

The weakness and how to handle it has provoked debate in the cryptography community. At issue: how much of the problem rests with email clients, versus fundamental issues with the PGP and S/MIME ecosystems generally. Some argue that clients should have acted on warning mechanisms like MDC, while others contend that interoperability was prioritized above a known threat for years.

"It should be patchable," says Matthew Green, a cryptographer at Johns Hopkins University. But, he adds, "People don’t pay attention unless there’s an attack."

As cryptographers continue to analyze the situation, some note that it should be possible to check encrypted inboxes for evidence of eFail attacks in the wild, by scanning for the suspicious HTML manipulations. And because of this detectability, some, like Dan Guido, CEO of the security firm Trail of Bits, note that the attack might not be so appealing to hackers in practice. "It doesn’t look like the team behind eFail researched possible detections or operational necessities for pulling off successful attacks," he says.

Until user services actually start issuing patches and scanning to see if the attack has been in use over the years, people looking to gain protection from encrypted email should lean on other types of secure communication or continue using encrypted email with knowledge of the risks. Mistakes are going to happen, but users would benefit from more cooperation and less in-fighting within the secure email community.

More Great WIRED Stories

- If Trump is laundering Russian money here's how it would work
- Spot the contraband in these airport baggage x-rays
- How a DNA transfer nearly convicted an innocent man of murder
- PHOTO ESSAY: Ominous views of Japan's new concrete seawalls
- Best robot vacuums: Pet hair, carpets, hardwood floors, and more

Related Video

Security

How to Get Started with Encrypted Messaging

It's 2017! It's time to start using an encrypted messaging app. Why? Using end-to-end encryption means that no one can see what you're sharing back and forth.