Major #eFail Vulnerability Exposes PGP Encrypted Email -- UPDATED

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digital and physical forms.

The public key of the encryption software GnuPG, an Open-Source-version of PGP. (Photo by Dünzlullstein bild via Getty Images)

Anyone using PGP to encrypt their email could have their messages exposed thanks to a severe vulnerability for which there's no proper fix. That's according to researchers in Germany, who said anyone using plug-ins allowing simple use of PGP should stop using them entirely and possibly delete them too.

The warning came from Sebastian Schinzel, lead of the IT security lab at the Münster University of Applied Sciences, who noted attacks exploiting the vulnerability "might reveal the plaintext of encrypted emails, including encrypted emails sent in the past." Though he isn't revealing the full details until Tuesday May 15, the findings have spooked security conscious folk.

Sebastian Schinzel
@seecurity

We'll publish critical vulnerabilities in PGP/GPG and S/MIME email encryption on 2018-05-15 07:00 UTC. They might reveal the plaintext of encrypted emails, including encrypted emails sent in the past. #efail 1/4

1,849 7:00 AM - May 14, 2018

2,467 people are talking about this

The Electronic Frontier Foundation (EFF) said it had reviewed the research and could "confirm that these vulnerabilities pose an immediate risk to those using these tools for email communication, including the potential exposure of the contents of past messages."

"Until the flaws described in the paper are more widely understood and fixed, 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," the EFF wrote in a blog post.

The EFF has also offered guidance on how to remove plug-ins associated with PGP email, which users can find in the blog. Those plug-ins include ones for clients Apple Mail, Thunderbird and Outlook.

It appears the vulnerability (which some have dubbed eFail) resides in such email clients, rather than a fundamental problem with the PGP standard, according to Werner Koch, the man behind GNUPrivacyGuard (GnuPG), the free and open source PGP software suite. In a post, Koch said he believed the EFF's comments on the issue were "overblown" and that he hadn't been contacted about the vulnerability.

@mikko @mikko · May 14, 2018
Replying to @mikko
This vulnerability might be used to decrypt the contents of encrypted emails sent in the past. Having used PGP since 1993,

this sounds baaad. #efail

GNU Privacy Guard
@gnupg

They figured out mail clients which don't properly check for decryption errors and also follow links in HTML mails. So the vulnerability is in the mail clients and not in the protocols. In fact OpenPGP is immune if used correctly while S/MIME has no deployed mitigation.

481 8:37 AM - May 14, 2018

472 people are talking about this

PGP was long seen as the standard for encrypted messaging and it remains the most popular method of sending private email. Increasingly, however, mobile apps like Signal, Apple's iMessage and Threema have provided simple methods for end-to-end encrypted communications.

Schinzel hadn't responded to a request for comment at the time of publication. He's done significant work on cryptographic weaknesses in the past; in 2016, he co-created an attack dubbed DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), which could decrypt people's web connections on 33 per cent of all HTTPS websites.

A trick to decrypt

The researchers explained in a website for the eFail vulnerability that it required the attacker to be able to intercept and email and tamper with it to reveal the plaintext of messages. "In a nutshell, eFail abuses active content of HTML emails, for example externally loaded images or styles, to exfiltrate plaintext through requested URLs," they wrote.

"The attacker changes an encrypted email in a particular way and sends this changed encrypted email to the victim. The victim's email client decrypts the email and loads any external content, thus exfiltrating the plaintext to the attacker."

The full technical paper is available here.

An old flaw

A spokesperson for ProtonMail, a webmail service that uses PGP, confirmed its services were not affected. The spokesperson also eFail wasn't exactly new. "It has

been known since 2001. The vulnerability exists in implementation errors in various PGP clients and not the protocol itself," the spokesperson added.

"What is newsworthy is that some clients that support PGP were not aware of this for 17 years and did not perform the appropriate mitigation.

"As the world's largest encrypted email service based on PGP, we are disappointed that some organizations and publications have contributed to a narrative that suggests PGP is broken or that people should stop using PGP. This is not a safe recommendation."

Apple gets fixing

An Apple spokesperson said partial fixes to eFail were released in iOS 11.3, which shipped March 29. The remaining fixes for affected Apple products being developed and will be with customers soon, they added.

Microsoft said it had no comment on the matter.

Got a tip? Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes. Email at TBrewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail.

Thomas Brewster Forbes Staff

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for Th...
Read More