Critical Flaws in PGP and S/MIME Tools Can Reveal Encrypted Emails in Plaintext

thehackernews.com/2018/05/pgp-smime-email-encryption.html

May 14, 2018

Note—the technical details of the vulnerabilities introduced in this article has now been released, so you should also read our latest article to learn how the eFail attack works and what users can do to prevent themselves.
An important warning for people using widely used email encryption tools—PGP and S/MIME—for sensitive communication.

A team of European security researchers has released a warning about a set of critical vulnerabilities discovered in PGP and S/Mime encryption tools that could reveal your encrypted emails in plaintext.

What's worse? The vulnerabilities also impact encrypted emails you sent in the past.

PGP, or Pretty Good Privacy, is an open source end-to-end encryption standard used to encrypt emails in a way that no one, not even the company, government, or cyber criminals, can spy on your communication.
S/MIME, Secure/Multipurpose Internet Mail Extensions, is an asymmetric cryptography-based technology that allows users to send digitally signed and encrypted emails.

Sebastian Schinzel, computer security professor at Münster University of Applied Sciences, headed on to Twitter to warn users of the issue, and said that "there are currently no reliable fixes for the vulnerability."

Electronic Frontier Foundation (EFF) has also confirmed the existence of “undisclosed” vulnerabilities and recommended users to uninstall PGP and S/MIME applications until the flaws are patched.

> "EFF has been in communication with the research team, and can 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," the organisation said in its blog post.

> "Our advice, which mirrors that of the researchers, is to immediately disable and/or uninstall tools that automatically decrypt PGP-encrypted email."

So, until the vulnerabilities are patched, users are advised to stop sending and especially reading PGP-encrypted emails for now, and use alternative end-to-end secure tools, such as Signal.
EFF has warned users to immediately disable if they have installed any of the following mentioned plugins/tools for managing encrypted emails:

- Thunderbird with Enigmail
- Apple Mail with GPGTools
- Outlook with Gpg4win

It should be noted that researchers have not claimed that the flaws reside in the way encryption algorithm works; instead, the issues appear in the way email decryption tools/plugins work.
The full technical details of the vulnerabilities will be released in a paper on Tuesday at 7 am UTC (3 am Eastern, midnight Pacific time).

Stay Tuned to The Hacker News for further details on the vulnerabilities.

Have something to say about this article? Comment below or share it with us onFacebook, Twitter or our LinkedIn Group.