Security

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

If a hacker can get into your inbox of ciphered messages, they may be able to read the content

By Shaun Nichols in San Francisco 14 May 2018 at 20:39 44 SHARE ▼

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 applications handle HTML content of these messages, an attacker could potentially see encrypted messages as plaintext.

The research team that uncovered the shortcomings claimed the only way to fully protect against EFAIL, right now, is to stop handling PGP and S/MIME decryption in your mail client, and fully patching it will require updates to the encryption standards themselves. Disabling the viewing of HTML content will help a lot in preventing decryption attacks. Even better, convert messages to plain text and read them offline in a text editor.

PGP and S/MIME decryptors can leak plaintext from emails, says infosec Professor

READ MORE

The vulnerability comes in two parts: an HTML exfiltration attack in which a snoop sends the target an email with specially crafted web mark-up language. The HTML code would then trick the victim's email client into fetching a URL with the unencrypted message contained in plain text in the request. The attacker would then simply need to find the URL request in their web server logs to see the decoded message.

The second component, referred to as CBC/CFB gadget attack, potentially allows an attacker to send malformed data blocks that, when read by the target, would fool the email client into sending to the attacker's server the unencrypted contents of the message.

The vulnerability has been assigned two CVE IDs. The PGP CFB gadget attack was assigned CVE-2017-17688, while the S/MIME CBC vulnerability was given CVE-2017-17689.

To mitigate the chance of a successful attack, users who rely on PGP or S/MIME for email encryption should disable the viewing of HTML emails, the eggheads stressed. That won't fully close the flaw, but it will cut off the primary way of exploiting it.

"The EFAIL attacks abuse active content, mostly in the form of HTML images, styles, etc," the researchers – Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky, and Jörg Schwenk – wrote.

"Disabling the presentation of incoming HTML emails in your email client

Don't panic, yet

There are also limitations to these attacks. The researchers said the gadget exploit technique is more effective for S/MIME than for PGP, where it only works about one third of the time.

The researchers also noted that an attacker needs full access to the target's email account, ie: the spy has to be able to log into your inbox. Unfortunately, guarding messages from an attacker with full access to your data is one of the primary use cases for both encryption formats.

So, basically, your email account needs to be hijacked first. For a well-protected inbox, using strong passwords and two-factor authentication using hardware tokens, this should be quite a challenge.

So, how bad is it? Hacker House cofounder and Brit infosec pro Matthew Hickey told *The Register* while we're unlikely to see widespread abuse of EFAIL, the potential for targeted attacks against journalists, corporations, activists, and academics makes it worth taking seriously.

"It's a serious risk if you rely on PGP and S/MIME for email security which most organisations use. It is not as severe as code execution and requires HTML emails to exploit so it may not be as wide spread for attacks," Hickey explained.

"It's still a concern, and our advice is to disable email plugins until a fix is supplied and disable HTML emails to prevent additional attack vectors."

Indeed, *El Reg* recommends opening PGP-encrypted emails in a text editor on a secured virtual machine, host, or container, depending on your level of paranoia, rather than allow encrypted HTML messages to be parsed and rendered. ®