Attention PGP Users: New Vulnerabilities Require You To Take Action Now

UPDATE: Enigmail and GPG Tools have been patched for EFAIL. For more up-to-date information, please see EFF's Surveillance Self-Defense guides.

UPDATE (5/14/18): More information has been released. See EFF's more detailed explanation and analysis here.

A group of European security researchers have released a warning about a set of vulnerabilities affecting users of PGP and S/MIME. 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 full details will be published in a paper on Tuesday at 07:00 AM UTC (3:00 AM Eastern, midnight Pacific). In order to reduce the short-term risk, we and the researchers have agreed to warn the wider PGP user community in advance of its full publication.

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

Please refer to these guides on how to temporarily disable PGP plug-ins in:

Thunderbird with Enigmail

Apple Mail with GPGTools

Outlook with Gpg4win

These steps are intended as a temporary, conservative stopgap until the immediate risk of the exploit has passed and been mitigated against by the wider community.

We will release more detailed explanation and analysis when more information is publicly available.