Critical PGP Security Issue

By *Roy Schestowitz*
Created *14/05/2018 - 7:06am*
Submitted by Roy Schestowitz on Monday 14th of May 2018 07:06:24 AM Filed under Security [1]

- **Attention PGP Users: New Vulnerabilities Require You To Take Action Now [2]**

  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.

- **Disabling PGP in Thunderbird with Enigmail [3]**

Security

Source URL: http://www.tuxmachines.org/node/111672

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-action-now

[3] https://www.eff.org/deeplinks/2018/05/disabling-pgp-thunderbird-enigmail