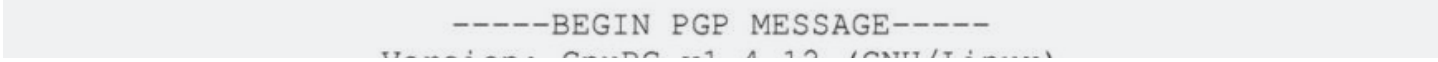
CAN'T GET NO RELIEF —

Critical PGP and S/MIME bugs can reveal encrypted emails—uninstall now [Updated]

The flaws can expose emails sent in the past and "pose an immediate threat."

DAN GOODIN - 5/14/2018, 8:02 AM



Elsamuko / Flickr

Enlarge

The research for this post is now public. See this post for details. A less drastic safeguard is to ensure HTML is disabled in the email client, although the researchers have warned that future exfiltration attacks may work even then. For the truly paranoid, disabling plugins that decrypt messages in the email client is the safest measure. In such scenarios, people can still encrypt and decrypt messages in a separate application. Again, see the latest post for more on this.

The Internet's two most widely used methods for encrypting email—PGP and S/MIME—are vulnerable to hacks that can reveal the plaintext of encrypted messages, a researcher warned late Sunday night. He went on to say there are no reliable fixes and to advise anyone who uses either encryption standard for sensitive communications to remove them immediately from email clients.

The flaws "might reveal the plaintext of encrypted emails, including encrypted emails you sent in the past," Sebastian Schinzel, a professor of computer security at Münster University of Applied Sciences, wrote on Twitter. "There are currently no reliable fixes for the vulnerability. If you use PGP/GPG or S/MIME for very sensitive communication, you should disable it in your email client for now."

Sebastian Schinzel @seecurity · May 14, 2018

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

Sebastian Schinzel
@seecurity

There are currently no reliable fixes for the vulnerability. If you use PGP/GPG or S/MIME for very sensitive communication, you should disable it in your email client for now. Also read @EFF's blog post on this issue: eff.org/deeplinks/2018… #efail 2/4

Attention PGP Users: New Vulnerabilities Require You To Tak…

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

eff.org

356 7:00 AM - May 14, 2018

489 people are talking about this

Schinzel referred people this blog post published late Sunday night by the Electronic Frontier Foundation. It said: "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 post continued:

> 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.

Both Schinzel and the EFF blog post referred those affected to EFF instructions for disabling plugins in Thunderbird, macOS Mail, and Outlook. The instructions say only to "disable PGP integration in e-mail clients." Interestingly, there's no advice to remove PGP apps such as Gpg4win or GNU Privacy Guard. Once the plugin tools are removed from Thunderbird, Mail, or Outlook, the EFF post said, "your emails will not be automatically decrypted." On Twitter, EFF officials went on to say: "do not decrypt encrypted PGP messages that you receive using your email client."

Little is publicly known about the flaws at the moment. Both Schinzel and the EFF blog post said they will be disclosed late Monday night California time in a paper written by a team of European security researchers. Schinzel's Twitter messages used the hashtag #efail, a possible indication of the name the researchers have given to their exploit.

FURTHER READING

More than 11 million HTTPS websites imperiled by new decryption attack

The research team members have been behind a variety of other important cryptographic attacks, including one from 2016 called Drown, which decrypted communications protected by the transport layer security protocol. Other researchers behind the PGP and S/MIME research include Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Simon Friedberger, juraj somorovsky, and Jörg Schwenk. Besides Münster University, the researchers also represent Ruhr-University and KU Leuven University.

Given the track record of the researchers and the confirmation from EFF, it's worth heeding the advice to disable PGP and S/MIME in email clients while waiting for more details to be released Monday night. Ars will publish many more details when they are publicly available.

Update: the paper detailing the "EFAIL" vulnerability was released early and is now available. We will be analyzing it this morning.

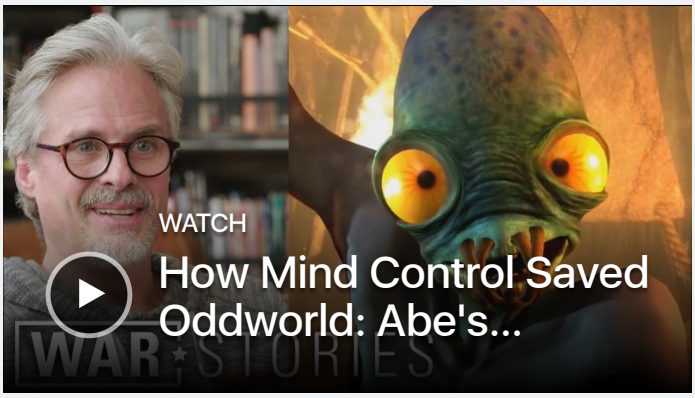
READER COMMENTS SHARE THIS STORY

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

CHANNEL ars



How Mind Control Saved Oddworld: Abe's Oddysee

When Lorne Lanning first conceived of what would become Oddworld, he wasn't necessarily setting out to make video games. What he needed to do was tell a story. On this episode of War Stories, we hear from the co-founder of Oddworld Inhabitants and learn all the ups and downs of Abe's journey to the screen over the past 22 years, including what comes next for the franchise in Oddworld: Soulstorm.

How Mind Control Saved Oddworld: Abe's Oddysee

Nintendo's Corey Olcsvary plays your Super Mario Maker 2 levels

Bioware answers unsolved mysteries of the Mass Effect universe

Civilization: It's good to take turns | War Stories

More videos

← PREVIOUS STORY

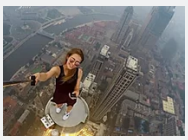
NEXT STORY →

Related Stories

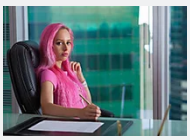
Sponsored Stories

Powered by outbrain

SmartWatch Everyone in Switzerland is Talking About
techgadgetdiscounts.com



Most Dangerous Selfies Ever Taken
Far and Wide



The 10 Highest Paying Jobs in Switzerland
Trendingstock Today

Switzerland: People Are Crazy About This New Fast-Selling Smartwatch
Next Tech

Switzerland : New Wifi Booster Stops Expensive Internet
techdiscountdeals.com

Esports in Education: Acer is ripe for disruption
Acer Blog

Today on Ars