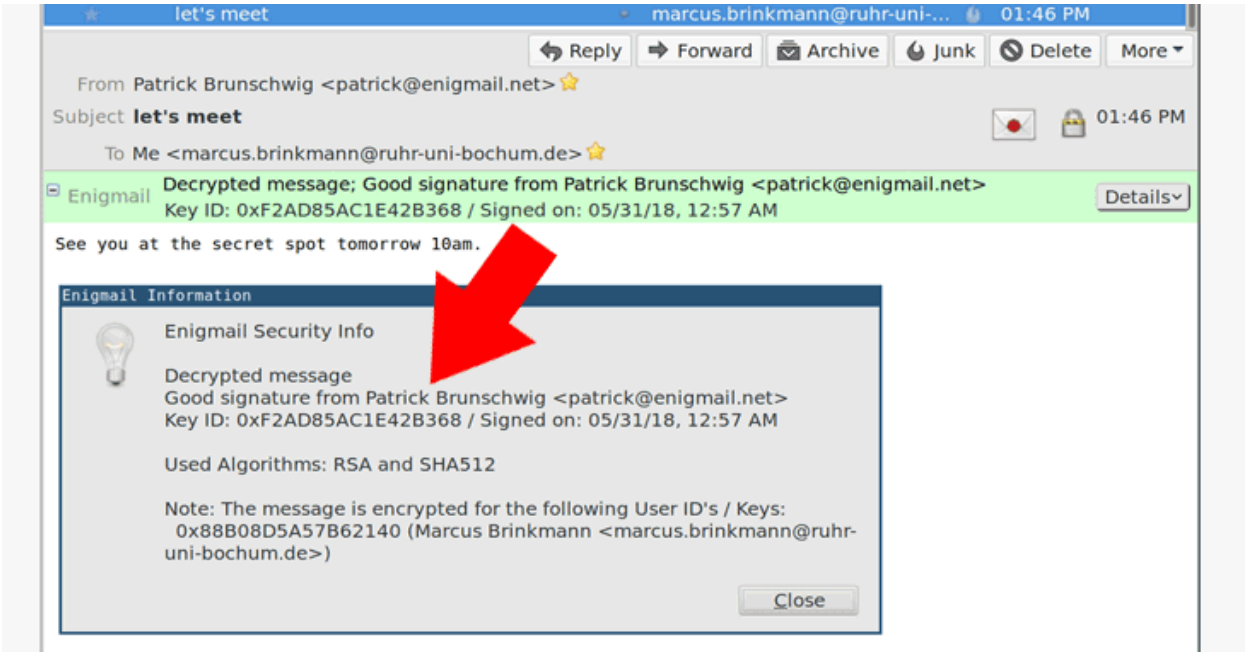
GnuPG Flaw in Encryption Tools Lets Attackers Spoof Anyone's Signature

thehackernews.com/2018/06/gnupg-encryption-signature.html

June 15, 2018



A security researcher has discovered a critical vulnerability in some of the world's most popular and widely used email encryption clients that use OpenPGP standard and rely on GnuPG for encrypting and digitally signing messages.
The disclosure comes almost a month after researchers revealed a series of flaws, dubbed **eFail**, in PGP and S/Mime encryption tools that could allow attackers to reveal encrypted emails in plaintext, affecting a variety of email programs, including Thunderbird, Apple Mail, and Outlook.

Software developer Marcus Brinkmann discovered that an input sanitization vulnerability, which he dubbed **SigSpoof**, makes it possible for attackers to fake digital signatures with someone's public key or key ID, without requiring any of the private or public keys involved.

The vulnerability, tracked as CVE-2018-12020, affects popular email applications including GnuPG, Enigmail, GPGTools and python-gnupg, and have now been patched in their latest available software updates.
As explained by the researcher, the OpenPGP protocol allows to include the "filename" parameter of the original input file into the signed or encrypted messages, combining it with the GnuPG status messages (including signature information) in a single data pipe (literal data packets) by adding a predefined keyword to separate them.

> "These status messages are parsed by programs to get information from gpg about the validity of a signature and other parameters," GnuPG maintainer Werner Koch said in an advisory published today.

During the decryption of the message at recipient's end, the client application splits up the information using that keyword and displays the message with a valid signature, if the user has the verbose option enabled in their gpg.conf file.

```
echo "See you at the secret spot tomorrow 10am." | gpg --
    armor --store --compress-level 0 --set-filename "`echo -
    ne \''\
\n[GNUPG:] GOODSIG F2AD85AC1E42B368 Patrick Brunschwig <
    patrick@enigmail.net>\
\n[GNUPG:] VALIDSIG F2AD85AC1E42B368 x 1527721037 0 4 0 1 10
    01\
\n[GNUPG:] TRUST_FULLY\
\n[GNUPG:] BEGIN_DECRYPTION\
\n[GNUPG:] DECRYPTION_OKAY\
\n[GNUPG:] ENC_TO 50749F1E1C02AB32 1 0\
\ngpg: '\''`" > poc2.msg
```

However, the researcher finds that the included file name, which can be up to 255 characters, does not properly get sanitized by the affected tools, potentially allowing an attacker to "include line feeds or other control characters in it."
Brinkmann demonstrates how this loophole can be used to inject arbitrary (fake) GnuPG status messages into the application parser in an attempt to spoof signature verification and message decryption results.

> "The attack is very powerful, and the message does not even need to be encrypted at all. A single literal data (aka 'plaintext') packet is a perfectly valid OpenPGP message, and already contains the 'name of the encrypted file' used in the attack, even though there is no encryption," Brinkmann says.

The researcher also believes that the flaw has the potential to affect "a large part of our core infrastructure" that went well beyond encrypted email, since "GnuPG is not only used for email security but also to secure backups, software updates in distributions, and source code in version control systems like Git."
Brinkmann also shared three proofs-of-concept showing how signatures can be spoofed in Enigmail and GPGTools, how the signature and encryption can be spoofed in Enigmail, as well as how a signature can be spoofed on the command line.

Since maintainers of three popular email clients have patched the issue, users are advised to upgrade their software to the latest versions.

If you are a developer, you are recommended to add --no-verbose" to all invocations of GPG and upgrade to python-gnupg 0.4.3.
Applications using GPGME as the crypto engine are safe. Also, GnuPG with --status-fd compilation flag set and --verbose flag not set are safe.

Share on Twitter

Technical Writer, Security Blogger and IT Analyst. She is a Technology Enthusiast with a keen eye on the Cyberspace and other tech related developments.

Latest Stories

Best Deals

Comments