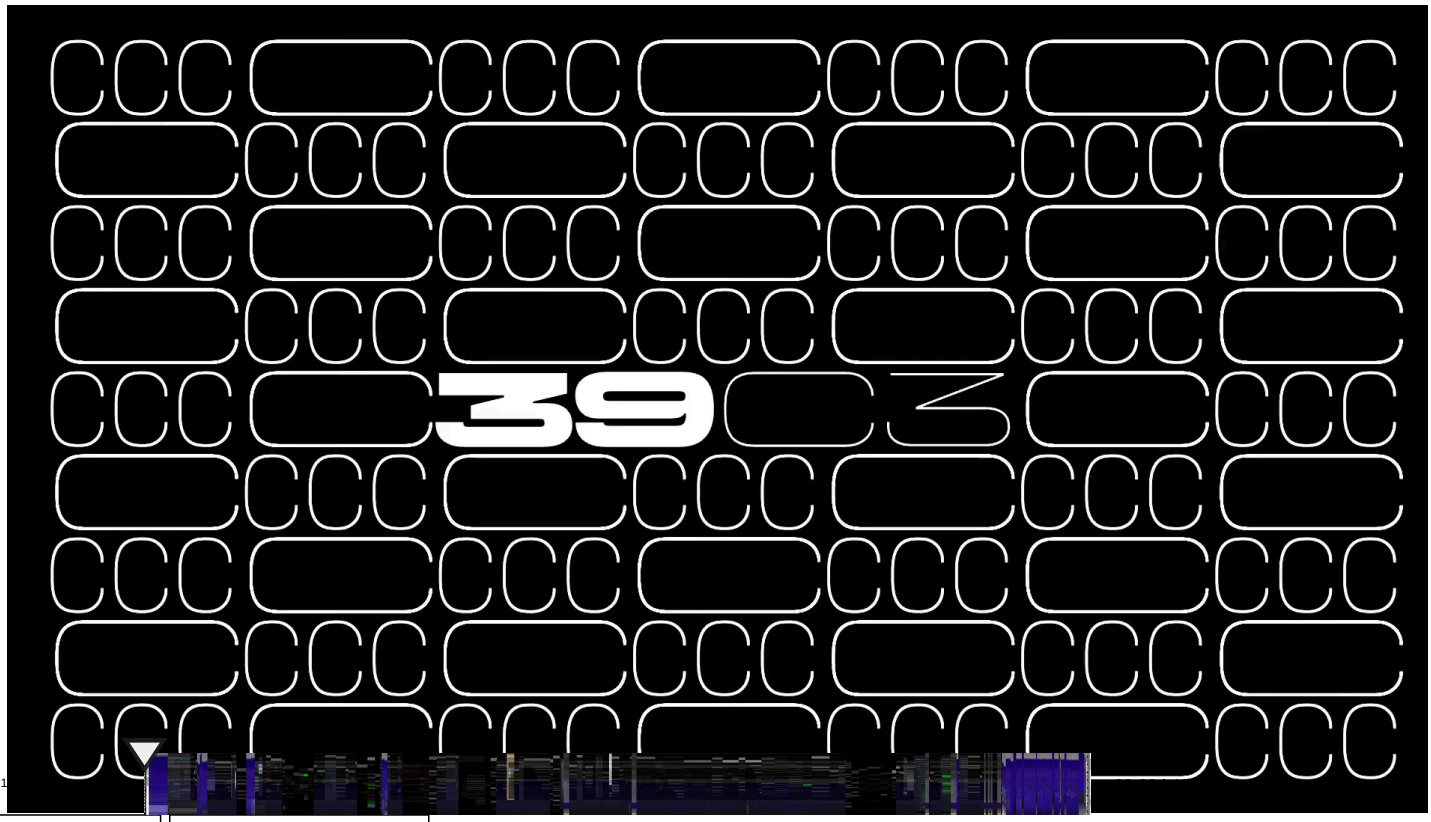
To sign or not to sign: Practical vulnerabilities in GPG & friends

(/c/39c3)

49016 (/search?p=49016) and Liam (/search?p=Liam)



One (/c/39c3/One) | Security (/c/39c3/Security) | Playlists: '39c3' videos starting here (/v/39c3-to-sign-or-not-to-sign-practical-vulnerabilities-i/playlist) / audio (/v/39c3-to-sign-or-not-to-sign-practical-vulnerabilities-i/audio)

48 min 2025-12-27 80.9k

Fahrplan (https://events.ccc.de/congress/2025/hub/event/detail/to-sign-or-not-to-sign-practical-vulnerabilities-i)

Might contain zerodays. https://gpg.fail/

From secure communications to software updates: PGP implementations such as *GnuPG* ubiquitously relied on to provide cryptographic assurances. Many applications fro secure communications to software updates fundamentally rely on these utilities.
Since these have been developed for decades, one might expect mature codebases, a multitude of code audit reports, and extensive continuous testing.
When looking into various PGP-related codebases for some personal use cases, we found these expectations not met, and discovered multiple vulnerabilities in cryptographi utilities, namely in *GnuPG*, *Sequoia PGP*, *age*, and *minisign*.
The vulnerabilities have implementation bugs at their core, for example in parsing code, rather than bugs in the mathematics of the cryptography itself. A vulnerability in a p could for example lead to a confusion about what data was actually signed, allowing attackers without the private key of the signer to swap the plain text. As we initially did r start with the intent of conducting security research, but rather were looking into understanding some internals of key management and signatures for personal use, we also discuss the process of uncovering these bugs. Furthermore, we touch on the role of the OpenPGP specification, and the disclosure process.

Beyond the underlying mathematics of cryptographic algorithms, there is a whole other layer of implementation code, assigning meaning to the processed data. For example signature verification operation both needs robust cryptography **and** assurance that the verified data is indeed the same as was passed into the signing operation. To faci the second part, software such as *GnuPG* implement parsing and processing code of a standardized format. Especially when implementing a feature rich and evolving stand there is the risk of ambivalent specification, and classical implementation bugs.

The impact of the vulnerabilities we found reaches from various signature verification bypasses, breaking encryption in transit and encryption at rest, undermining key signat to exploitable memory corruption vulnerabilities.

Download

Video

AV1 MP4 WebM

Download 1080p

eng-deu-fra 395 MB (https://cdn.media.ccc.de/congress/2025/av1-hd/39c3-1854-eng-deu-fra-To_sign_or_not_to_sign_Practical_vulner

These files contain multiple languages.

This Talk was translated into multiple languages. The files available for download contain all languages as separate audio-tracks. Most desktop video players allow you to choose between them.

Please look for "audio tracks" in your desktop video player.

Subtitles

eng
(https://static.media.ccc.de/media/congress/2025/1854-e448ef16-47cf-57ad-9fbd-a5f91aa4aa3b-eng.vtt)

Help us to improve these subtitles! (https://www.c3subtitles.de/talk/guid/e448ef16-47cf-57ad-9fbd-a5f91aa4aa3b)

Audio

Download mp3

eng 44 MB (https://cdn.media.ccc.de/congress/2025/mp3/39c3-1854-eng-To_sign_or_not_to_sign_Practical_vulnerabilities_in_GPG_frie

Download mp3

deu 44 MB (https://cdn.media.ccc.de/congress/2025/mp3-translated/39c3-1854-deu-To_sign_or_not_to_sign_Practical_vulnerabilities_i

Download opus

eng 30 MB (https://cdn.media.ccc.de/congress/2025/opus/39c3-1854-eng-To_sign_or_not_to_sign_Practical_vulnerabilities_in_GPG_frie

Download opus

deu 31 MB (https://cdn.media.ccc.de/congress/2025/opus-translation/39c3-1854-deu-To_sign_or_not_to_sign_Practical_vulnerabilities_

Embed

<iframe width="1024" height="576" src="https://media.ccc.de/v/39c3-to-sign-or-not-to-sign-practical-vulnerabilities-i/oembed" frameborder="0" allowfullscreen></ifrar

Share:

Tags

1854 (/tags/1854) 2025 (/tags/2025) 39c3 (/tags/39c3) Security (/c/39c3/Security) One (/c/39c3/One) 39c3-eng (/tags/39c3-eng) 39c3-deu (/tags/39c3-deu) 39c3-fra (/tags/39c3-fra) Day 1 (/c/39c3/Day%201)