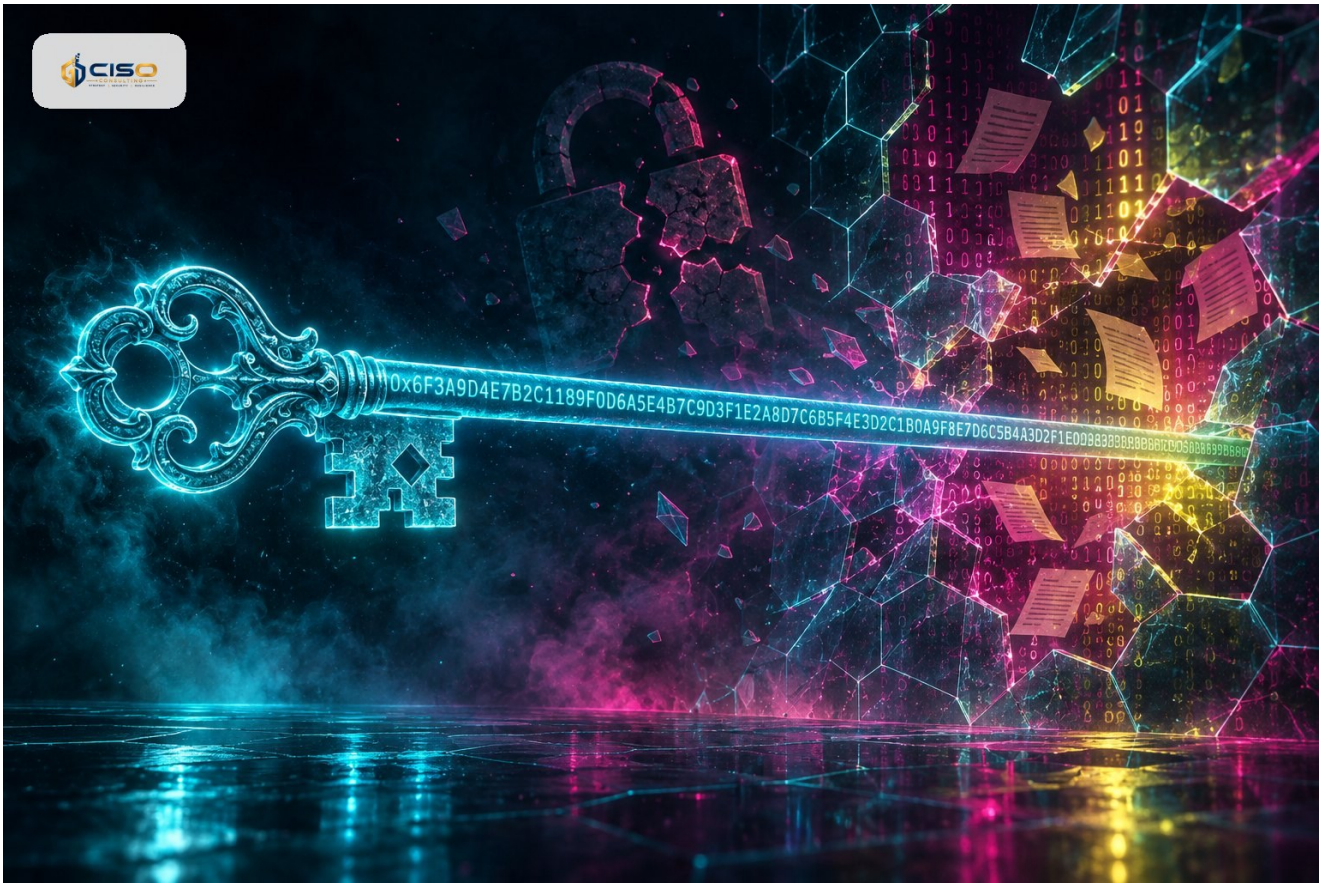
GnuPG Warns of Critical GPGME Flaw Triggered by Malicious OpenPGP Keys



GnuPG reports a critical memory bug in GPGME, CVE-2026-129975, triggered by an OpenPGP key with an unusually long user ID. It could expose application data; GPGME 2.3.0 contains the fix.

- The flaw is tracked as CVE-2026-129975 and is rated critical.
- A malicious OpenPGP key with an unusually long user ID can trigger the memory bug.
- It could be used to steal data from affected applications.
- All software using GPGME before version 2.3.0 is affected.
- The GnuPG project has released fixed versions.

The GnuPG project has warned of a critical memory bug in GPGME, the standard library that programs use to work with GnuPG. The issue is tracked as CVE-2026-129975.

What is affected

A malicious OpenPGP key carrying an unusually long user ID can trigger the flaw. According to the project, this could be used to steal data from applications that rely on the library. The bug affects all software that uses GPGME in versions before 2.3.0. The project has released fixed versions.

Because GPGME is a library rather than a standalone product, exposure may not be obvious. Applications that handle encryption, signing or key import through GnuPG may include it, directly or as a dependency.

What to do next

The source does not describe active exploitation, so the priority is orderly inventory and patching rather than emergency action. Institutions should identify where GPGME is used, upgrade to version 2.3.0 or later, and be careful with OpenPGP keys from untrusted sources until systems are updated.

Where an application bundles its own copy of the library, the fix will usually depend on the application vendor, so ask suppliers to confirm their status.

What to do now

1. Inventory applications, servers and tools that use GPGME or GnuPG, including indirect dependencies.
2. Upgrade GPGME to version 2.3.0 or later, prioritising internet-facing and data-handling systems.
3. Ask software vendors that bundle GPGME to confirm whether their products are affected and when fixes will ship.
4. Avoid importing OpenPGP keys from untrusted sources until patching is complete.
5. Record the vulnerability and remediation in your vulnerability management process.