GnuPG VS-Desktop - Version 3.1.26 (en)

g10 Code GmbH

2022-12-14

GnuPG VS-Desktop version 3.1.26 is available since 2022-12-14. The previous version was 3.1.25. 3.1.26 is a security update and part of the regular release schedule.

Notes to Admins

Another security bug has been found in libksba, the library used by GnuPG for parsing the ASN.1 structures as used by S/MIME. The bug affects all versions of libksba before 1.6.3 and may be used for remote code execution when processing a rogue CRLs. For a description see the bug report T6284. **Please update to this new version as soon as possible**.

New Features

GUI (Kleopatra)

- New Option to delete the locally stored secret key after a transfer to a smart card. (T5836)
- Improve the display of keys in the group edit dialog. (T6295)
- Simplify changing the owner trust of keys. (T6148)
- Allow selecting ECC with supported curves when generating new keys on smart cards. (T4429)
- Support the import of non-standard conforming UTF-16 encoded text files with certificates. (T6298)

Engine (GnuPG)

- Improve signature verification speed by a factor of more than four. Double detached signing speed. (T5826)
- Add a notation to new encryption subkeys in de-vs mode. (T6279)
- Import stray revocation certificates to improve WKD usability.
- New option –add-revocs for gpg-wks-client.
- Ignore expired user-ids in gpg-wks-client. (T6292)
- Make –require-compliance work without the –status-fd option.
- Support the Telesec Signature Card v2.0 in OpenPGP. (T6252)

Solved Bugs

GUI (Kleopatra)

- Exit without error message if a key signing job was canceled. (T6305)
- Report failed imports immediately when receiving the result. (T6302)
- Do not offer invalid S/MIME certificates for signing or encryption. (T6216)
- Don't ask user to certify an imported expired or revoked OpenPGP key. (T6155)
- Do not crash when closing details widget while certificate dump is shown. (T6180)
- Improve usability and accessibility of the notepad operations. (T6188)

Outlook Add-In (GgpOL)

- IMAP access to encrypted mails works again. (T6203)

Engine (GnuPG)

- Update the X.509/CMS library Libksba to version 1.6.3 to fix a security problem in the CRL signature parser. (T6230)
- Fix trusted introducer for mbox only user-ids. (T6238)

Versions of the Components

Component	Version	Remarks
GnuPG	2.2.41	T6280
Kleopatra	3.1.26	
GpgOL	2.5.6-beta5	
GpgEX	1.0.9	
Libgcrypt	1.8.9	
Libksba	1.6.3	