GnuPG VS-Desktop - Version 3.1.25 (en)

g10 Code GmbH

2022-10-17

GnuPG VS-Desktop version 3.1.25 is available since 2022-10-14. The previous version was 3.1.24. 3.1.25 is a security update outside of the regular release schedule and contains only a few new features in the engine.

Notes to Admins

A severe 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 1.6.2 and may be used for remote code execution. **Updating to this new version is thus important**.

For the detailed description please see our security advisory. This is CVE-2022-3515.

New Features

Engine (GnuPG)

- GnuPG: In de-vs mode use AES-128 instead of 3-DES as implicit preference. This avoids problems with software considering 3-DES as non-compliant but only announcing 3-DES as supported algorithm. (T6063)
- GnuPG: Add new LDAP server flag "areconly" (A-record-only) to help against long delays on some AD installations.
- GnuPG: New feature to mirror an LDAP keyserver to a Web Key Directory. (T6224)
- GnuPG: Improve reporting of bad passphrase errors during PKCS#11 import. (T5713,T6037)

Solved Bugs

Engine (GnuPG)

- GnuPG: Update the X.509/CMS parsing library libksba to version 1.6.2 to fix a severe security problem. (T6230)
- GnuPG: Do not consider unknown public keys as non-compliant while decrypting. (T6205)
- GnuPG: Fix CRL Distribution Point fallback to other schemes.
- GnuPG: Fix upload of multiple keys for an LDAP server specified using the colon format.
- GnuPG: Fix a key upload problem when a BaseDN is specified for an LDAP server. (T6047)

Versions of the Components

Component	Version	Remarks
GnuPG	2.2.40	T6181
Kleopatra	3.1.24	
GpgOL	2.5.4	
GpgEX	1.0.9	
Libgcrypt	1.8.9	