# GnuPG VS-Desktop - Version 3.1.25 (de)

g10 Code GmbH

2022-10-17

GnuPG VS-Desktop ist seit 2022-10-14 in der Version 3.1.25 verfügbar. Die vorherige Version war 3.1.24. 3.1.25 wurde als Sicherheitsupdate außerhalb des regulären Release Plans veröffentlicht und enthält nur wenige neue Features in der GnuPG-engine.

## Hinweise an die Administratorinnen

Es wurde ein schwerer Fehler in libksba gefunden, der Bibliothek, die GnuPG für das Parsen der von S/MIME genutzten ASN.1 Strukturen verwendet. Der Fehler betrifft alle Versionen von libksba vor Version 1.6.2 und kann für Remote Code Execution benutzt werden. **Ein Update auf diese neue Version ist daher wichtig**.

Für mehr Details siehe unser Security Advisory. (CVE-2022-3515)

## Neue Features

### Engine (GnuPG)

- GnuPG: Im VS-NfD Modus wird jetzt AES-128 anstatt 3-DES als implizierter Verschlüsselungsalgorithmus verwendet. Dies vermeidet Probleme mit Software, die 3-DES als nicht nicht konform ansieht obgleich sie lediglich 3-DES als unterstützten Algorithmus publiziert. (T6063)

- GnuPG: Das neue LDAP Server Flag "areconly" (A-record-only) kann benutzt werden, um lange Verzögerungen auf einigen AD Installationen zu vermeiden.

- GnuPG: Ein neues Feature ermöglicht das Spiegeln der Schlüssel eines internen LDAP Keyservers auf ein Web Key Directory. (T6224)

- GnuPG: Die Fehlermeldung bei falscher Passworteingabe beim Import von PKCS#11 Daten wurde verbessert. (T5713,T6037)

## Behobene Fehler

### Engine (GnuPG)

- GnuPG: Die X.509/CMS Parser DLL libksba wurde auf Version 1.6.2 aktualisiert um ein gravierendes Sicherheitsproblem zu beheben. (T6230)
- GnuPG: Unbekannte Schlüssel werden bei der Entschlüsselung nicht mehr als nicht-konform angesehen. (T6205)
- GnuPG: Der Rückgriff auf andere CRL Distribution Points im Fehlerfall wurde verbessert.
- GnuPG: Das Hochladen von mehreren Schlüsseln auf LDAP Server, die im "colon" Format konfiguriert sind, funktioniert jetzt.
- GnuPG: Das Hochladen von Schlüsseln auf einen LDAP Server mit konfigurierter BaseDN funktioniert jetzt. (T6047)

## Versionen der Komponenten

| Komponente | Version | Anmerkungen |
|---|---|---|
| GnuPG | 2.2.40 | T6181 |
| Kleopatra | 3.1.24 | |
| GpgOL | 2.5.4 | |
| GpgEX | 1.0.9 | |
| Libgcrypt | 1.8.9 | |