GnuPG VS-Desktop - Version 3.1.26 (de)

g10 Code GmbH

2022-12-14

GnuPG VS-Desktop ist seit 2022-12-14 in der Version 3.1.26 verfügbar. Die vorherige Version war 3.1.25. 3.1.26 wurde als Sicherheitsupdate innerhalb des regulären Release Plans veröffentlicht.

Hinweise an die Administratorinnen

Ein weiteres Sicherheitsproblem wurde 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 1.6.6 und kann für Remote Code Execution benutzt werden, wenn eine speziell präparierte CRL überprüft wird. Eine Beschreibung finden Sie im Fehlerbericht T6284. **Bitte aktualisieren Sie sobald als möglich auf diese Version**.

Neue Features

GUI (Kleopatra)

- Neue Option um den lokal gespeicherten geheimen Schlüssel nach der Übertragung auf eine Smartcard zu löschen. (T5836)
- Im Dialog zur Einrichtung von Gruppen wurde die Darstellung von Schlüsseln verbessert. (T6295)
- Der Dialog zur Änderung der Vertrauenswürdigkeit des Besitzers wurde vereinfacht. (T6148)
- Bei der Generierung von Schlüsseln auf Smartcards werden jetzt auch unterstützte ECC Kurven angeboten. (T4429)

- Der Import von Zertifikaten aus nicht Standard konformen UTF-16 kodierten Textdateien ist nun möglich. (T6298)

Engine (GnuPG)

- Die Überprüfung von Signaturen ist jetzt viermal schneller. Das Signieren ist jetzt doppelt so schnell. (T5826)
- Neue Unterschlüssel zur Verschlüsselung haben im de-vs Modus jetzt eine Notation, um deren Verwaltung zukünftig zu vereinfachen. (T6279)
- Zusätzlich eingefügte Revocation Zertifikate werden jetzt mit importiert, um das WKD zu verbessern.
- Das Programm gpg-wks-client hat jetzt eine neue Option –add-revocs.
- Das Programm gpg-wks-client ignoriert jetzt abgelaufene User IDs. (T6292)
- Die Option –require-compliance funktioniert jetzt auch ohne die Verwendung der Option –status-fd.
- Die Telesec Signature Card v2.0 wird jetzt für OpenPGP unterstützt. (T6252)

Behobene Fehler

GUI (Kleopatra)

- Es wird kein Fehler mehr angezeigt, wenn die Beglaubigung eines Schlüssels abgebrochen wurde. (T6305)
- Fehler beim Import werden jetzt direkt angezeigt. (T6302)
- S/MIME Zertifikate, die zum Signieren oder Verschlüsseln nicht gültig sind, werden nicht mehr angeboten. (T6216)
- Die Benutzerin wird nicht mehr gefragt, ob sie ein importiertes aber abgelaufenes oder widerrufenes OpenPGP Zertifikat beglaubigen möchte. (T6155)
- Ein Absturz nach dem Schließen eines Details Dialogs wurde behoben. (T6180)

- Kleopatra: Verbesserungen an der Barrierefreiheit des Notizblocks. (T6188)

Outlook Add-In (GgpOL)

- Der IMAP Zugriff auf verschlüsselte Mails funktioniert wieder. (T6203)

Engine (GnuPG)

- Die X.509/CMS DLL Libksba wurde auf Version 1.6.3 aktualisiert um ein Sicherheitsproblem im Parser von CRL Signaturen zu beheben. (T6230)

- Trusted Introducer funktionieren jetzt auch, wenn die User-ID nur aus einer Mailadresse besteht (T6238)

Versionen der Komponenten

Komponente	Version	Anmerkungen
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	