



CVE-2022-26306

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-26306 |
| State | PUBLIC |
| Assigner | security@documentfoundation.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-07-25 15:15:00 UTC |
| Updated | 2023-07-11 14:35:00 UTC |
| Description | LibreOffice supports the storage of passwords for web connections in the user's configuration database. The stored passwords |

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------|--------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Application | Libreoffice | Libreoffice | All | All | All | All |

References

Reference

- [SECURITY] [DLA 3368-1] libreoffice security update
- CVE-2022-26306 | LibreOffice - Free Office Suite - Based on OpenOffice - Compatible with Microsoft
- oss-security - CVE-2022-37400: Apache OpenOffice Static Initialization Vector Allows to Recover Passwords for Web Connections Without Knowledge of Password
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160422 Oracle Enterprise Linux Security Update for libreoffice (ELSA-2023-0304)

181023 Debian Security Update for libreoffice (CVE-2022-26306)

101000 Debian Security Update for libreoffice (DLA 3368-1)

| |
|--|
| 181639 Debian Security Update for libreoffice (DLA 3368-1) |
| 198976 Ubuntu Security Notification for LibreOffice Vulnerabilities (USN-5661-1) |
| 199000 Ubuntu Security Notification for LibreOffice Vulnerabilities (USN-5694-1) |
| 241056 Red Hat Update for libreoffice (RHSA-2023:0089) |
| 241115 Red Hat Update for libreoffice (RHSA-2023:0304) |
| 376798 LibreOffice Multiple Vulnerabilities |
| 502565 Alpine Linux Security Update for libreoffice |
| 502588 Alpine Linux Security Update for libreoffice |
| 940875 AlmaLinux Security Update for libreoffice (ALSA-2023:0089) |
| 940908 AlmaLinux Security Update for libreoffice (ALSA-2023:0304) |
| 960556 Rocky Linux Security Update for libreoffice (RLSA-2023:0304) |
| 960559 Rocky Linux Security Update for libreoffice (RLSA-2023:0089) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)