Security

If you came here looking for end-user support, please send any questions **not** related to a specific security bug to users@global.libreoffice.org.

The security teams for products associated with the codebase can be contacted at officesecurity@lists.freedesktop.org - this includes representatives of many vendors, and associated projects. This email address is **solely** for reporting security issues related to the software. If your **virus checker** is flagging a LibreOffice download as containing a virus, this is almost certainly a **false positive.** Please check with another anti-virus vendor, and/or file a bug report with them before bothering the security list. Also please consider purchasing a more accurate virus checker.

In your report, please include the following information:

1. In what version did you identify the specific security problem
2. If it is platform dependent, which platform are you using
3. A proof of concept if possible

Please note that bugs which cause the application to crash, but are otherwise un-exploitable are not treated as security vulnerabilities, and finders are encouraged to diagnose and contribute fixes to recent versions of LibreOffice in the normal way.

Incident Response Procedure

1. You privately share the details of the security vulnerability with our Security Team by emailing officesecurity@lists.freedesktop.org

2. We acknowledge your submission and verify the vulnerability. Our first answer generally comes under 48 hours.
3. Our policy is to disclose the vulnerability to the public within 30 days of resolution of the issue
4. Reports will be credited in security advisories, but reporters may remain anonymous if they wish.

Security Advisories

Addressed in LibreOffice 26.2.3/25.8.7

▶ CVE-2026-4430 Heap Buffer Overflow in AgileEngine

Addressed in LibreOffice 25.2.4/25.8.0

▶ CVE-2025-14714 TCC Bypass via Inherited Permissions in Bundled Interpreter

Addressed in LibreOffice 24.8.6/25.2.2

▶ CVE-2025-2866 PDF signature forgery with adbe.pkcs7.sha1 SubFilter

Addressed in LibreOffice 24.8.5/25.2.1

▶ CVE-2025-1080 Macro URL arbitrary script execution

Addressed in LibreOffice 24.8.5

▶ CVE-2025-0514 Executable hyperlink Windows path targets executed unconditionally on activation

Addressed in LibreOffice 24.8.4

▶ CVE-2024-12425 Path traversal leading to arbitrary .ttf file write
▶ CVE-2024-12426 URL fetching can be used to exfiltrate arbitrary INI file values and environment variables

Addressed in LibreOffice 24.8.0/24.2.5

▶ CVE-2024-7788 Signatures in "repair mode" should not be trusted

Addressed in LibreOffice 24.2.5

▶ CVE-2024-6472 Ability to trust not validated macro signatures removed in high security mode

Addressed in LibreOffice 24.2.4

▶ CVE-2024-5261 TLS certificate are not properly verified when utilizing LibreOfficeKit

Addressed in LibreOffice 7.6.7/24.2.3

▶ CVE-2024-3044 Graphic on-click binding allows unchecked script execution

Addressed in LibreOffice 7.6.4/7.5.9

▶ CVE-2023-6186 Link targets allow arbitrary script execution

Addressed in LibreOffice 7.6.3/7.5.9

▶ CVE-2023-6185 Improper input validation enabling arbitrary Gstreamer pipeline injection

Addressed in LibreOffice 7.4.7/7.5.3

▶ CVE-2023-2255 Remote documents loaded without prompt via IFrame

Addressed in LibreOffice 7.4.6/7.5.1

▶ CVE-2023-0950 Array Index UnderFlow in Calc Formula Parsing

Addressed in LibreOffice 7.3.6/7.4.1

▶ CVE-2022-3140 Macro URL arbitrary script execution

Addressed in LibreOffice 7.2.7/7.3.3

▶ CVE-2022-26306 Static Initialization Vector Allows to Recover Passwords for Web Connections Without Knowing the Master Password

▶ CVE-2022-26307 Weak Master Keys

Addressed in LibreOffice 7.2.7/7.3.2

▶ CVE-2022-26305 Execution of Untrusted Macros Due to Improper Certificate Validation

Addressed in LibreOffice 7.2.6/7.3.1

▶ CVE-2022-38745 Empty entry in Java class path risks arbitrary code execution

Addressed in LibreOffice 7.2.5/7.3.0

▶ CVE-2021-25636 Incorrect trust validation of signature with ambiguous KeyInfo children

Addressed in LibreOffice 7.0.6/7.1.3

▶ CVE-2021-25632 fileloc extension added to macOS executable denylist

Addressed in LibreOffice 7.0.6/7.1.2

▶ CVE-2021-25633 Content Manipulation with Double Certificate Attack

▶ CVE-2021-25634 Timestamp Manipulation with Signature Wrapping

Addressed in LibreOffice 7.0.5/7.1.2

▶ CVE-2021-25631 Denylist of executable filename extensions possible to bypass under windows

Addressed in LibreOffice 7.0.5/7.1.1

▶ CVE-2021-25635 Content Manipulation with Certificate Validation Attack

Addressed in LibreOffice 6.4.4

▶ CVE-2020-12802 remote graphics contained in docx format retrieved in 'stealth mode'
▶ CVE-2020-12803 XForms submissions could overwrite local files

Addressed in LibreOffice 6.3.6/6.4.3

▶ CVE-2020-12801 Crash-recovered MSOffice encrypted documents defaulted to not to using encryption on next save

Addressed in LibreOffice 6.2.7/6.3.1

▶ CVE-2019-9854 Unsafe URL assembly flaw in allowed script location check
▶ CVE-2019-9855 Windows 8.3 path equivalence handling flaw allows LibreLogo script execution

Addressed in LibreOffice 6.2.6/6.3.1

▶ CVE-2019-9853 Insufficient URL decoding flaw in categorizing macro location

Addressed in LibreOffice 6.2.6/6.3.0

▶ CVE-2019-9850 Insufficient url validation allowing LibreLogo script execution
▶ CVE-2019-9851 LibreLogo global-event script execution
▶ CVE-2019-9852 Insufficient URL encoding flaw in allowed script location check

Addressed in LibreOffice 6.2.5

▶ CVE-2019-9848 LibreLogo arbitrary script execution
▶ CVE-2019-9849 remote bullet graphics retrieved in 'stealth mode'

Addressed in LibreOffice 6.1.6/6.2.3

▶ CVE-2019-9847 Executable hyperlink targets executed unconditionally on activation

Addressed in LibreOffice 6.0.7/6.1.3

▶ CVE-2018-16858 Directory traversal flaw in script execution

Addressed in LibreOffice 5.4.7/6.0.4

▶ CVE-2018-10583 Information disclosure via SMB link embedded in ODF document

Fixed in LibreOffice 5.4.6/6.0.2

▶ CVE-2018-10120 Heap Buffer Overflow in MSWord Customizations parsing

Fixed in LibreOffice 5.4.5/6.0.1

▶ CVE-2018-1055 Remote arbitrary file disclosure vulnerability via WEBSERVICE formula
▶ CVE-2018-10119 Use After Free in Structured Storage parser

Fixed in LibreOffice 5.2.5/5.3.0

▶ CVE-2017-7870 Heap-buffer-overflow in WMF filter
▶ CVE-2016-10327 Heap-buffer-overflow in EMF filter

Fixed during development

▶ CVE-2017-7856 Heap-buffer-overflow in SVM filter
▶ CVE-2017-7882 Heap-buffer-overflow in HWP filter
▶ CVE-2017-8358 Heap-buffer-overflow in JPG filter

Fixed in LibreOffice 5.1.6/5.2.2/5.3.0

▶ CVE-2017-3157 Arbitrary file disclosure in Calc and Writer

Fixed in LibreOffice 5.1.4/5.2.0

▶ CVE-2016-4324 Dereference of invalid STL iterator on processing RTF file

Fixed in LibreOffice 5.0.5/5.1.0

▶ CVE-2016-0795 LotusWordPro Bounds overflows in LwpTocSuperLayout processing

Fixed in LibreOffice 5.0.4/5.1.0

- CVE-2016-0794 LotusWordPro Multiple bounds overflows in lwp filter

Fixed in LibreOffice 5.0.2/5.1.0

- CVE-2017-12607 Out-of-Bounds Write in Impress' PPT Filter
- CVE-2017-12608 Out-of-Bounds Write in Writer's ImportOldFormatStyles

Fixed in LibreOffice 4.4.6/5.0.1

- CVE-2015-5214 DOC Bookmark Status Memory Corruption

Fixed in LibreOffice 4.4.5/5.0.0

- CVE-2015-4551 Arbitrary file disclosure in Calc and Writer
- CVE-2015-5212 ODF Integer Underflow (PrinterSetup Length)
- CVE-2015-5213 DOC piecetable Integer Overflow

Fixed in LibreOffice 4.3.7/4.4.2

- CVE-2015-1774 Out of bounds write in HWP file filter

Fixed in LibreOffice 4.2.7/4.3.3

- CVE-2014-3693 Use-After-Free in socket manager of Impress Remote

Fixed in LibreOffice 4.2.6-secfix/4.3.1

- CVE-2014-3524 CSV Command Injection and DDE formulas
- CVE-2014-3575 Arbitrary File Disclosure using crafted OLE objects

Fixed in LibreOffice 4.2.5

- CVE-2014-0247 Microsoft Office VBA Macro Execution

Fixed in LibreOffice 3.6.7

▶ CVE-2013-4156 Microsoft .docm Denial Of Service

Fixed in LibreOffice 3.5.7

▶ CVE-2012-4233 Multiple file format denial of service vulnerabilities

Fixed in LibreOffice 3.5.5

▶ CVE-2012-2665 Multiple heap-based buffer overflows in the XML manifest encryption handling code

Fixed in LibreOffice 3.5.3

▶ CVE-2012-1149 Integer overflows in graphic object loading
▶ CVE-2012-2334 Integer overflow flaw with malformed PPT files

Fixed in LibreOffice 3.4.6/3.5.1

▶ CVE-2012-0037 XML Entity Expansion flaw by processing RDF file

Fixed in LibreOffice 3.4.3:

▶ CVE-2011-2713 Multiple vulnerabilities in the 'Microsoft Word' (doc) binary file format importer
▶ CVE-2013-2189 Microsoft .doc Memory Corruption Vulnerability
▶ CVE-2017-9806 Out-of-Bounds Write in Writer's WW8Fonts Constructor

Fixed in LibreOffice 3.3.3/3.4.0:

▶ CVE-2011-2685 Multiple vulnerabilities in the 'Lotus Word Pro' (lwp) file format importer

Third Party Advisories

Fixed in LibreOffice 4.2.3

▶ CVE-2014-0160 & more (a set of vulnerabilities) TLS heartbeat read overrun (4.1 line not affected)

Fixed in LibreOffice 4.1.5/4.2.0

▶ CVE-2013-1752 &CVE-2013-4238 Python Multiple Vulnerabilities

Fixed in all versions

▶ CVE-2018-14939 overflow at realpath, not a bug in LibreOffice

▶ CVE-2012-2149 libwpd: Memory overwrite flaw by processing certain WordPerfect (WPD). No version of LibreOffice is affected by this.

Security

Credits

Get Help

FAQ

Community Assistance

Documentation

Installation Instructions

System Requirements

Professional Support

Accessibility

Community

Join Us - Start Here!

Events

Blog

Read Our Blog

DONATE

Language: English (US)

Follow us!

Contact Us Datenschutzerklärung (Privacy Policy) Impressum (Legal Info)

Trademarks Statutes (non-binding English translation)

Satzung (binding German version)