



CVE-2017-7870

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-7870
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-14 04:59:00 UTC
Updated	2018-01-05 02:31:00 UTC
Description	LibreOffice before 2017-01-02 has an out-of-bounds write caused by a heap-based buffer overflow related to the tools::Poly

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libreoffice	Libreoffice	All	beta2	All	All

References

Reference	Source	Link
LibreOffice: Multiple vulnerabilities (GLSA 201706-28) — Gentoo security	GENTOO	security.gentoo.org
Red Hat Customer Portal	REDHAT	access.redhat.com
372 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org
CVE-2017-7870 LibreOffice - Free Office Suite - Fun Project - Fantastic People	CONFIRM	www.libreoffice.org
ofz#372 check if ImplSplit succeeded · LibreOffice/core@62a97e6 · GitHub	MISC	github.com
LibreOffice CVE-2017-7870 Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com
Debian -- Security Information -- DSA-3837-1 libreoffice	DEBIAN	www.debian.org
LibreOffice Heap Overflow in tools::Polygon::Insert() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

[710560](#) Gentoo Linux LibreOffice Multiple Vulnerabilities (GLSA 201706-28)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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