



# CVE-2023-32700

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-32700
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-20 18:15:00 UTC
<b>Updated</b>	2023-11-07 04:14:00 UTC
<b>Description</b>	LuaTeX before 1.17.0 allows execution of arbitrary shell commands when compiling a TeX file obtained from an untrusted s

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Luatex Project</a>	<a href="#">Luatex</a>	All	All	All	All
Application	<a href="#">Miktex</a>	<a href="#">Miktex</a>	All	All	All	All
Application	<a href="#">Tug</a>	<a href="#">Tex Live</a>	All	All	All	All

## References

Reference	Source	Link
luatex-1.17.0 update - tex-live mailing list - TeX Users Group	MISC	<a href="https://tug.org">tug.org</a>
[SECURITY] Fedora 37 Update: texlive-base-20210325-54.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.</a>
1.17.0 · Tags · TeXLive / luatex · GitLab	MISC	<a href="https://gitlab.lisn.upsaclay">gitlab.lisn.upsaclay</a>
[SECURITY] Fedora 38 Update: texlive-base-20220321-72.fc38 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.</a>
Release Rebuild TL2023 for luatex · TeX-Live/texlive-source · GitHub	MISC	<a href="https://github.com">github.com</a>
LuaTeX Security Vulnerabilities	MISC	<a href="https://tug.org">tug.org</a>
[SECURITY] Fedora 38 Update: texlive-base-20220321-72.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.</a>
[SECURITY] Fedora 37 Update: texlive-base-20210325-54.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160747](#) Oracle Enterprise Linux Security Update for texlive (ELSA-2023-3661)

[181792](#) Debian Security Update for texlive-bin (DSA 5406-1)

[181793](#) Debian Security Update for texlive-bin (DLA 3427-1)

[181817](#) Debian Security Update for texlive-bin (DLA 3427-2)

[184915](#) Debian Security Update for texlive-bin (CVE-2023-32700)

[199373](#) Ubuntu Security Notification for TeX Live Vulnerability (USN-6115-1)

[241727](#) Red Hat Update for texlive (RHSA-2023:3661)

[284013](#) Fedora Security Update for texlive (FEDORA-2023-d261122726)

[284095](#) Fedora Security Update for texlive (FEDORA-2023-38094d905c)

[503270](#) Alpine Linux Security Update for texlive

[506258](#) Alpine Linux Security Update for texlive

[754037](#) SUSE Enterprise Linux Security Update for texlive (SUSE-SU-2023:2285-1)

[754040](#) SUSE Enterprise Linux Security Update for cups-filters, poppler, texlive (SUSE-SU-2023:2287-1)

[941149](#) AlmaLinux Security Update for texlive (ALSA-2023:3661)

[960944](#) Rocky Linux Security Update for texlive (RLSA-2023:3661)

© [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](#)