



CVE-2020-17354

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-17354
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-15 22:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	LilyPond before 2.24 allows attackers to bypass the -dsafe protection mechanism via output-def-lookup or output-def-scope

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lilypond	Lilypond	All	All	All	All

References

Reference	Source	Link
Debian Package Tracker	MISC	tracker.debian.org
[SECURITY] Fedora 37 Update: lilypond-doc-2.24.1-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
LilyPond – Music notation for everyone: Download	MISC	lilypond.org
Remove safe mode (!1522) · Merge requests · LilyPond / LilyPond · GitLab	CONFIRM	gitlab.com
[SECURITY] Fedora 36 Update: lilypond-doc-2.24.1-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 37 Update: lilypond-doc-2.24.1-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Extension:Score/2021 security advisory - MediaWiki	MISC	www.mediawiki.org
LilyPond Application Usage: 1.2 Command-line usage	MISC	lilypond.org
[SECURITY] Fedora 36 Update: lilypond-doc-2.24.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Login	MISC	phabricator.wikimedia.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[283940](#) Fedora Security Update for lilypond (FEDORA-2023-fb8bc496c2)

[283941](#) Fedora Security Update for lilypond (FEDORA-2023-6edb8fab0d)

© [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](#)