



CVE-2020-23903

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

Summary

CVE	CVE-2020-23903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-10 22:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A Divide by Zero vulnerability in the function static int read_samples of Speex v1.2 allows attackers to cause a denial of ser

Risk And Classification

Problem Types: CWE-369

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Xiph	Speex	1.2	-	All	All

References

Reference	Source	Link
speexenc encode wav file dos vulnerability · Issue #13 · xiph/speex · GitHub	MISC	github.com
[SECURITY] Fedora 35 Update: mingw-speex-1.2.0-9.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: mingw-speex-1.2.0-9.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: mingw-speex-1.2.0-9.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 35 Update: mingw-speex-1.2.0-9.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.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

160312 Oracle Enterprise Linux Security Update for speex (ELSA-2022-7979)
198662 Ubuntu Security Notification for Speex Vulnerability (USN-5280-1)
240877 Red Hat Update for speex (RHSA-2022:7979)
282090 Fedora Security Update for mingw (FEDORA-2021-73c086ef46)
282142 Fedora Security Update for mingw (FEDORA-2021-91f16837bf)
296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)
671567 EulerOS Security Update for speex (EulerOS-SA-2022-1552)
671680 EulerOS Security Update for speex (EulerOS-SA-2022-1765)
751419 SUSE Enterprise Linux Security Update for speex (SUSE-SU-2021:3858-1)
751434 OpenSUSE Security Update for speex (openSUSE-SU-2021:3860-1)
751466 OpenSUSE Security Update for speex (openSUSE-SU-2021:1538-1)
940802 AlmaLinux Security Update for speex (ALSA-2022:7979)
960546 Rocky Linux Security Update for speex (RLSA-2022:7979)

© [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](#)