



CVE-2021-3826

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

Summary

CVE	CVE-2021-3826
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-01 21:15:00 UTC
Updated	2024-01-22 15:01:00 UTC
Description	Heap/stack buffer overflow in the dlang_lname function in d-demangle.c in libiberty allows attackers to potentially cause a d

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Gnu	Gcc	11.2	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: insight-13.0.50.20220502-1.fc35 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
gcc.gnu.org Git - gcc.git/commit	MISC	gcc.gnu.org
[SECURITY] Fedora 36 Update: mingw-gcc-11.2.1-6.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
[SECURITY] Fedora 35 Update: insight-13.0.50.20220502-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
[SECURITY] Fedora 36 Update: mingw-gdb-12.1-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
gcc.gnu.org Git	MISC	gcc.gnu.org
[SECURITY] Fedora 36 Update: mingw-gdb-12.1-2.fc36 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
[SECURITY] Fedora 37 Update: mingw-binutils-2.38-5.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
[SECURITY] Fedora 37 Update: mingw-binutils-2.38-5.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
[PATCH] libiberty: prevent null dereferencing on dlang_type	MISC	gcc.gnu.org

[SECURITY] Fedora 36 Update: mingw-gcc-11.2.1-6.fc36 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
[SECURITY] Fedora 36 Update: mingw-binutils-2.37-5.fc36 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
[SECURITY] Fedora 36 Update: mingw-binutils-2.37-5.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
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

- [161078](#) Oracle Enterprise Linux Security Update for gdb (ELSA-2023-6372)
- [182579](#) Debian Security Update for libibertybinutils (CVE-2021-3826)
- [241553](#) Red Hat Update for devtoolset-12-binutils (RHSA-2023:3269)
- [242296](#) Red Hat Update for gdb (RHSA-2023:6372)
- [283099](#) Fedora Security Update for insight (FEDORA-2022-8e1df11a7a)
- [283289](#) Fedora Security Update for mingw (FEDORA-2022-19538a3732)
- [283290](#) Fedora Security Update for mingw (FEDORA-2022-affcf9eea6)
- [283299](#) Fedora Security Update for mingw (FEDORA-2022-c9a1fd5370)
- [283446](#) Fedora Security Update for mingw (FEDORA-2022-667ee398b1)
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [752893](#) SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2022:4146-1)
- [752941](#) SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2022:4277-1)
- [941376](#) AlmaLinux Security Update for gdb (ALSA-2023:6372)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report