

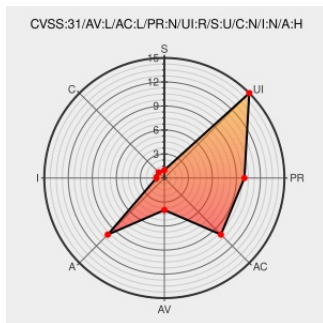


CVE-2019-14274

Published on: 07/25/2019 12:00:00 AM UTC

Last Modified on: 12/13/2022 02:25:00 PM UTC

CVE-2019-14274

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mcpp](#) from [Mcpp Project](#) contain the following vulnerability:

MCP 2.7.2 has a heap-based buffer overflow in the do_msg() function in support.c.

CVE-2019-14274 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:0382-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0382
[security-announce] openSUSE-SU-2020:0391-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0391

libmcpp: Denial of service (GLSA 202208-04) — Gentoo security

security.gentoo.org

text/html

GENTOO GLSA-202208-04

mcpp / Bugs / #13 Multiple Heap-based Buffer Overflow in the do_msg() function

Exploit

Third Party Advisory

sourceforge.net

text/html

MISC

sourceforge.net/p/mcpp/bugs/13/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

710578

Gentoo Linux libmcpp Denial of service Vulnerability (GLSA 202208-04)

901073

Common Base Linux Mariner (CBL-Mariner) Security Update for mcpp (6679)

906322

Common Base Linux Mariner (CBL-Mariner) Security Update for mcpp (6679-2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcpp Project	Mcpp	2.7.2	All	All	All
Application	Mcpp Project	Mcpp	2.7.2	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
cpe:2.3:a:mcpp_project:mcpp:2.7.2:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:mcpp_project:mcpp:2.7.2:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:opensuse:backports_sle:15.0:sp1:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:leap:15.1:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →