VDB-356620 · CVE-2026-6042 · GCVE-100-356620

MUSL LIBC UP TO 1.2.6 GB18030 4-BYTE DECODER SRC/LOCALE/ICONV.C ICONV ALGORITHMIC COMPLEXITY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$5k	1.55-

Summary

A vulnerability described as problematic has been identified in musl libc up to 1.2.6. Affected by this vulnerability is the function `iconv` of the file *src/locale/iconv.c* of the component *GB18030 4-byte Decoder*. Executing a manipulation can lead to algorithmic complexity. This vulnerability is registered as CVE-2026-6042. The attack needs to be launched locally. No exploit is available. It is advisable to implement a patch to correct this issue.

Details

A vulnerability has been found in musl libc up to 1.2.6 and classified as problematic. This vulnerability affects the function `iconv` of the file *src/locale/iconv.c* of the component *GB18030 4-byte Decoder*. The manipulation with an unknown input leads to a algorithmic complexity vulnerability. The CWE definition for the vulnerability is CWE-407. An algorithm in a product has an inefficient worst-case computational complexity that may be detrimental to system performance and can be triggered by an attacker, typically using crafted manipulations that ensure that the worst case is being reached. As an impact it is known to affect availability.

The advisory is shared for download at openwall.com. This vulnerability was named CVE-2026-6042. The exploitation appears to be easy. The attack needs to be approached locally. There are known technical details, but no exploit is available.

It is declared as highly functional.

Applying a patch is able to eliminate this problem. The bugfix is ready for download at openwall.com.

Similar entries are available at VDB-67432, VDB-68352, VDB-73110 and VDB-170494.

Product

Vendor

- musl

Name

- libc

Version

- 1.2.0
- 1.2.1
- 1.2.2
- 1.2.3
- 1.2.4
- 1.2.5
- 1.2.6

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.3
VulDB Meta Temp Score: 3.2

VulDB Base Score: 3.3
VulDB Temp Score: 3.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Vendor Base Score (musl): 🔒
Researcher Base Score: 🔒

Exploiting

Class: Algorithmic complexity
CWE: CWE-407 / CWE-404
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: Yes

Availability: 🔒
Status: Highly functional
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Patch
Status: 🔍

0-Day Time: 🔒

Patch: openwall.com

Timeline

04/09/2026		Advisory disclosed
04/09/2026	+0 days	VulDB entry created
04/09/2026	+0 days	VulDB entry last update

Sources

Advisory: openwall.com
Status: Confirmed

CVE: CVE-2026-6042 (🔒)
GCVE (CVE): GCVE-0-2026-6042
GCVE (VulDB): GCVE-100-356620
See also: 🔒

Entry

Created: 04/09/2026 07:39 PM
Updated: 04/09/2026 07:58 PM
Changes: 04/09/2026 07:39 PM (55), 04/09/2026 07:55 PM (20), 04/09/2026 07:58 PM (2)
Complete: 🔍
Submitter: 0x001
Committer: 0x001
Cache ID: 20:EC6:179

Submit

Accepted

- Submit #796352: musl libc musl 0.8.0 - 1.2.6 Inefficient Algorithmic Complexity (by 0x001)

Discussion

No comments yet. Languages: en.

Please log in to comment.