VDB-356989 · CVE-2026-6125 · IHURVQ

DROMARA WARM-FLOW UP TO 1.8.4 WORKFLOW DEFINITION /WARM-FLOW/SAVE-JSON SPELHELPER.PARSEEXPRESSION LISTENERPATH/SKIPCONDITION/PERMISSIONFLAG CODE INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.98-

Summary

A vulnerability has been found in Dromara warm-flow up to 1.8.4 and classified as critical. The affected element is the function `SpelHelper.parseExpression` of the file */warm-flow/save-json* of the component *Workflow Definition Handler*. This manipulation of the argument *listenerPath/skipCondition/permissionFlag* causes code injection. The identification of this vulnerability is CVE-2026-6125. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability has been found in Dromara warm-flow up to 1.8.4 and classified as critical. Affected by this vulnerability is the function `SpelHelper.parseExpression` of the file */warm-flow/save-json* of the component *Workflow Definition Handler*. The manipulation of the argument `listenerPath/skipCondition/permissionFlag` with an unknown input leads to a code injection vulnerability. The CWE definition for the vulnerability is CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at gitee.com. This vulnerability is known as CVE-2026-6125. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1059 for this issue.

It is possible to download the exploit at gitee.com. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- Dromara

Name

- warm-flow

Version

- 1.8.0
- 1.8.1
- 1.8.2
- 1.8.3
- 1.8.4

Website

- Product: https://gitee.com/dromara/warm-flow/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

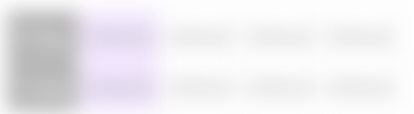
VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒



Threat Intelligence

Interest: 🔍
Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/11/2026	+0 days	VulDB entry last update

Sources

Product: gitee.com

Advisory: IHURVQ
Status: Not defined

CVE: CVE-2026-6125 (🔒)
GCVE (CVE): GCVE-0-2026-6125
GCVE (VulDB): GCVE-100-356989
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/11/2026 10:25 PM
Changes: 04/11/2026 10:25 PM (58)
Complete: 🔍
Submitter: anch0r
Cache ID: 68:9DC:179

Submit

Accepted

- Submit #793322: Dromara warm-flow <= 1.8.4 Code Injection (by anch0r)

Discussion

No comments yet. Languages: en.

Please log in to comment.