COMMUNITY CONTENT

Home › Submit › 793322

Submit #793322: Dromara warm-flow <= 1.8.4 Code Injection

Title	Dromara warm-flow <= 1.8.4 Code Injection
Description	A vulnerability was found in Dromara warm-flow up to version 1.8.4. The SpelHelper.parseExpression() method in the warm-flow-plugin-modes-sb module uses an unsandboxed StandardEvaluationContext to evaluate SpEL expressions. Malicious SpEL expressions can be injected into the listenerPath, skipCondition, and permissionFlag fields of a workflow definition via the /warm-flow/save-json endpoint. When a workflow instance is triggered, the injected expressions are executed, leading to Remote Code Execution (RCE). The exploit has been disclosed to the vendor.
Source	⚠ https://gitee.com/dromara/warm-flow/issues/IHURVQ
User	anch0r (UID 96691)
Submission	03/31/2026 04:19 AM (12 days ago)
Moderation	04/11/2026 10:20 PM (12 days later)
Status	Accepted
VulDB entry	[Dromara warm-flow up to 1.8.4 Workflow Definition /warm-flow/save-json SpelHelper.parseExpression listenerPath/skipCondition/permissionFlag code injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling