Remote Code Execution (RCE) vulnerability in dropwizard-validation <2.0.2

High joschi published GHSA-3mcp-9wr4-cjqf on Feb 24, 2020

Package

dropwizard-validation (Maven)

Affected versions	Patched versions
<1.3.19, <2.0.2	1.3.19, 2.0.2

Description

Summary

A server-side template injection was identified in the self-validating (`@SelfValidating`) feature of **dropwizard-validation** enabling attackers to inject arbitrary Java EL expressions, leading to Remote Code Execution (RCE) vulnerability.

If you're using a self-validating bean (via `@SelfValidating`), an upgrade to Dropwizard 1.3.19 or 2.0.2 is strongly recommended.

Impact

This issue may allow Remote Code Execution (RCE), allowing to run arbitrary code on the host system (with the privileges of the Dropwizard service account privileges) by injecting arbitrary Java Expression Language (EL) expressions when using the self-validating feature (`@SelfValidating` , `@SelfValidation`) in **dropwizard-validation**.

Patches

The issue has been fixed in **dropwizard-validation 1.3.19** and **2.0.2**. We strongly recommend upgrading to one of these versions.

Workarounds

If you are not able to upgrade to one of the aforementioned versions of **dropwizard-validation** but still want to use the `@SelfValidating` feature, make sure to properly sanitize any message you're adding to the `ViolationCollector` in the method annotated with `@SelfValidation` .

Example:

```
@SelfValidation
public void validateFullName(ViolationCollector col) {
    if (fullName.contains("_")) {
        // Sanitize fullName variable by escaping relevant characters such as "$"
        col.addViolation("Full name contains invalid characters:  " + sanitizeJavaEl(fullName));
    }
}
```

See also:
https://github.com/dropwizard/dropwizard/blob/v2.0.2/dropwizard-validation/src/main/java/io/dropwizard/validation/selfvalidating/ViolationCollector.java#L84-L98

References

- #3157
- #3160
- https://docs.oracle.com/javaee/7/tutorial/jsf-el.htm
- https://docs.jboss.org/hibernate/validator/6.1/reference/en-US/html_single/#section-interpolation-with-message-expressions
- https://beanvalidation.org/2.0/spec/#validationapi-message-defaultmessageinterpolation

For more information

If you have any questions or comments about this advisory:

- Open an issue in dropwizard/dropwizard
- Start a discussion on the dropwizard-dev mailing list

Security contact

If you want to responsibly disclose a security issue in Dropwizard or one of its official modules, please contact us via the published channels in our security policy:

https://github.com/dropwizard/dropwizard/security/policy#reporting-a-vulnerability

Severity

High

CVE ID

CVE-2020-5245

Weaknesses

No CWEs

Credits

pwntester