New issue

Jump to bottom

GHSL-2020-021 - Bypass input sanitization of EL expressions #155

Closed **mpiggott** opened this issue on Apr 14, 2021 · 4 comments · Fixed by #160

Labels bug **Component: Impl** **Priority: Critical** vulnerability

mpiggott commented on Apr 14, 2021

Github posted this publicly about 2-weeks ago - https://securitylab.github.com/advisories/GHSL-2020-021-jakarta-el/

5

erlioniel commented on Apr 15, 2021

Hello,
As a library user I would like to hear some info about how the team is suppose to handle the vulnerability. Is there any plans to react & fix the issue?

Br.
Vladimir

1

markt-asf commented on Apr 15, 2021 Contributor

Here is everything I know.

This was reported to the Eclipse security team on 2020-04-14. The EL project lead was informed via being CC'd on the BugZilla issue on 2020-04-20. I don't know if the EL project lead received that email or whether it was lost in a spam filter etc. I haven't been able to identify any further activity at Eclipse since then. You need to be an Eclipse committer to access that issue but (AFAICT) there isn't any information there that isn't in the published report or this comment.

I found out about this issue via $work a couple of days ago. As a Tomcat committer I wanted to check whether Tomcat was also vulnerable since the Jakarta EL implementation was originally forked from Tomcat. Tomcat was fixed in a commit some time ago. That fix may not apply directly to Jakarta EL as there have been other fixes to Tomcat's EL parsing grammar since the fork.

The Tomcat fixes are available to the Jakarta EL project under the ALv2.

The main focus of my time is Apache Tomcat. My work at Jakarta is on the specifications and the APIs. I simply don't have the time to maintain the Jakarta implementations as well.

For folks that need an immediate fix, my recommendation would be to use a different implementation where the issue has been fixed / doesn't exist. The benefit of the Java EE / Jakarta EE specs is that you should be able to freely switch implementations.

1

markt-asf added bug **Component: Impl** **Priority: Critical** labels on Apr 15, 2021

waynebeaton commented on May 26, 2021

I've assigned CVE-2021-28170 and have pushed a report to the central authority. I will continue to monitor this issue and push updates to the report as requested by the project team.

waynebeaton added the vulnerability label on May 26, 2021

joschi added a commit to dropwizard/dropwizard that referenced this issue on Jun 19, 2021

`Add test cases for deferred EL expressions` ... ✓ 99c483c

set-leanix mentioned this issue on Jun 28, 2021

"Improper Input Validation" security risk through dropwizard-validation > jakarta.el dropwizard/dropwizard#4091

Closed

This was referenced on Jun 29, 2021

ELParserTokenManager enables invalid EL expressions to be evaluate jbossas/el-ri#2

Merged

CVE-2021-28170 Fix expression delimiter escaping #160

Merged

TomasHofman commented on Jul 1, 2021 Contributor

Proposed PR: #160

m0mus closed this as completed in #160 on Aug 16, 2021

This was referenced on Aug 17, 2021

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar - autoclosed lukebrogan-mend/WebGoat#77
Closed

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar Yoavmartin/spring-petclinic#16
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar Tim-sandbox/WebGoat#45
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar gms-ws-sandbox/WebGoat8#128
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar Tim-sandbox/webgoat-trng#128
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar rsoreq/cwa-server#25
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar LynRodWS/alcor#96
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar RG4421/atlasdb#246
Open

CVE-2021-28170 (Medium) detected in jakarta.el-3.0.3.jar gms-ws-sandbox/dev-example-places#74
Open

strehle mentioned this issue on Aug 21, 2021

Eclipse Jakarta Expression Language library needs version bump cloudfoundry/uaa#1653
Closed

strehle mentioned this issue on Sep 2, 2021

update jakarta.el CVE-2021-28170 spring-projects/spring-boot#27861
Closed

strehle added a commit to strehle/spring-boot that referenced this issue on Sep 2, 2021

`update jakarta.el CVE-2021-28170` ··· `1c7390d`

jycr mentioned this issue on Jan 19

CVE-2021-28170 on jakarta.el-api-3.0.3 (transitive dependency of quarkus-core) quarkusio/quarkus#23003
Closed

Assignees

No one assigned

Labels

bug Component: Impl Priority: Critical vulnerability

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

CVE-2021-28170 Fix expression delimiter escaping
TomasHofman/el-ri

5 participants