July 15, 2020

GHSL-2020-043: Server-side template injection in Liferay - CVE-2020-13445

Alvaro Munoz

Summary

A user with privileges to edit FreeMarker or Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running Liferay.

Note: The follwing sandbox escape techniques have been tested on Liferay Portal WebContent templates and Liferay Portal Dynamic Data List Display templates, but it should work on other FreeMarker/Velocity templates used across all Liferay products (eg: DXP, Commerce, etc.)

Product

Liferay Portal CE

Tested Version

Liferay Portal CE, version 7.3 GA1

Details

Server-Side Template Injection (FreeMarker)

Even though Liferay does a good job extending the FreeMarker sandbox with a custom ObjectWrapper (`com.liferay.portal.template.freemarker.internal.RestrictedLiferayObjectWrapper.java`) which enhances which objects can be accessed from a Template, and also disables insecure defaults such as the `?new` built-in to prevent instantiation of arbitrary classes, it stills exposes a number of objects through the Templating API that can be used to circumvent the sandbox and achieve remote code execution.

Deep inspection of the exposed objects' object graph allows an attacker to get access to objects that allow them to instantiate arbitrary Java objects.

Server-Side Template Injection (Velocity)

Liferay also uses Velocity templates for Dynamic Data Lists Display. We can use similar vectors on Velocity templates.

Impact

This issue may lead to `Remote Code Execution`.

CVE

CVE-2020-13445

Coordinated Disclosure Timeline

This report was subject to the GHSL coordinated disclosure policy.

- 03/23/2020: Sent report to security@liferay.com
- 03/25/2020: Issue is acknowledged
- 05/27/2020: Fix is released as part of Liferay Portal 7.3.2

Credit

This issue was discovered and reported by GHSL team member @pwntester (Alvaro Munoz).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2020-043` in any communication regarding this issue.