Security Advisory 2020-022

Liferay Portal – Exploited Remote Code Execution Vulnerabilities

April 17, 2020 — v1.0

TLP:WHITE

History:

- *17/04/2020 — v1.0 – Initial publication*

Summary

On March 20, 2020, **Code White** released two proof-of-concepts for vulnerabilities on Liferay Portal [1]. These vulnerabilities were patched by Liferay [2]. However, CERT-EU is aware of these vulnerabilities being actually exploited by malicious threat actors to gain illicit access to unpatched exposed servers.

This second vulnerability is massively scanned for exploitation [5] and CERT-EU is aware of ongoing campaigns exploiting this vulnerability as several proof of concept are available online [6]. It is strongly recommended to check the version of Liferay portal being used and look for traces of intrusion on the potentially impacted servers.

Technical Details

The vulnerabilities concern JSON deserialization, allowing remote code execution on the target. The first vulnerability (CST-7111) [3] was reported in December 2018 and is due to a flaw in the `Flexjson` library. The second vulnerability (CST-7205/CVE-2020-7961) [4] was reported in June 2019 and is due to a flaw in the library replacing the `Flexjson` library (`Jodd Json`). In this case, one of the calls allows variable type definition making it possible for a dangerous method to be called, ultimately leading to remote code execution.

Deserialization vulnerabilities are due to structured data being rebuild into an object in a faulty manner, allowing an attacker to inject malicious code on the target when the object is rebuild.

The first vulnerability is located in the `Flexjson` library used for serializing and deserializing. The insecure feature allow specifying the class to deserialize within the JSON data itself.

The second vulnerability is due to two insecure features:

- In the `Jodd Json` library, one call allows in `JSONWebServiceActionParameters` user-set types (`parameterType`).

- The `JSONWebServiceActionParameters` object is passed to a web service call of Liferay Portal where the typename is used. By using a specially crafted json object, any type can be specified and so any method can be invoked.

Products Affected

- Liferay Portal versions 6.1
- Liferay Portal versions 6.2
- Liferay Portal versions 7.0
- Liferay Portal versions 7.1
- Liferay Portal versions 7.2

Recommendations

Check the patch level of servers using Liferay Portal. The following versions contain the patches:

- Liferay Portal versions 6.2 GA6
- Liferay Portal versions 7.0 GA7
- Liferay Portal versions 7.1 GA4
- Liferay Portal versions 7.2 GA2

In case the server was vulnerable at some point of time (especially after March 20, 2020), it is also recommended to check the following events:

- Unusual access to JSON web service API (`/api/jsonws`).
- In application logs, check for execution of `getRuntime().exec()` .
- If end-point logs are available, check unusual process being spawned by Java binaries.

References

[1] https://codewhitesec.blogspot.com/2020/03/liferay-portal-json-vulns.html

[2] https://liferay.dev/blogs/-/blogs/security-patches-for-liferay-portal-6-2-7-0-and-7-1

[3] https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/113765197

[4] https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/117954271

[5] https://twitter.com/bad_packets/status/1244866189408362498

[6] https://github.com/mzer0one/CVE-2020-7961-POC