CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-010

Oracle WebLogic 0-day Vulnerability

April 29, 2019 — v1.1

TLP:WHITE

History:

- *26/04/2019 — v1.0 – Initial publication*
- *29/04/2019 — v1.1 – Update: Oracle patch*

Summary

A highly critical, zero-day vulnerability in Oracle WebLogic server was disclosed. Some attackers might have already started exploiting it in the wild [1, 2, 3]. The vulnerability potentially allows attackers to remotely execute arbitrary commands. Oracle has issued an out-of-band security update to address this vulnerability.

Technical Details

Oracle WebLogic is a Java-based enterprise application server. It is used both in cloud and traditional environments. The application server contains a critical *deserialization* vulnerability that can lead to remote code execution. It affects all versions of the software. The vulnerability received the identification number CVE-2019-2725 [5].

It appears that vulnerability in `wls9_async` and `wls-wsat` components may allow deserialization of malicious code, which could lead to remote command execution. The first component adds support for server asynchronous operations, while the second is the server's security component. The vulnerability was described by the researchers from **KnownSec 404** in [1], and it allows attackers to remotely execute arbitrary commands on the affected servers by sending a specially crafted HTTP request, without requiring any authorization [2].

Products Affected

This vulnerability affects all WebLogic versions (including the latest version) that have the `wls9_async_response.war` and `wls-wsat.war` components enabled.

Recommendations

Oracle has issued an out-of-band security update to address this vulnerability for the supported versions (10.3.6.0.0 and 12.1.3.0.0). It is recommended to use the patch as soon as possible. More details are provided in [4].

Alternatively, if using the patch is not immediately possible, there are so far two mitigation techniques that have been identified:

- Find and delete: `wls9_async_response.war` and `wls-wsat.war`. Restart the WebLogic service[1].
- Restrict HTTP access for the `/_async/*` and `/wls-wsat/*` URL paths (by access policy control, web application firewall, etc.).

References

[1] https://medium.com/@knownseczoomeye/knownsec-404-team-oracle-weblogic-deserialization-rce-vulnerability-0day-alert-90dd9a79ae93

[2] https://thehackernews.com/2019/04/oracle-weblogic-hacking.html

[3] https://www.zdnet.com/article/new-oracle-weblogic-zero-day-discovered-in-the-wild/

[4] https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

[5] https://blogs.oracle.com/security/security-alert-cve-2019-2725-released

[1] Note that this could impact the functionality, if these components are used.