CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-037

Critical Vulnerabilities in Oracle WebLogic Server

July 22, 2021 — v1.0

TLP:WHITE

History:

- *22/07/2021 — v1.0 – Initial publication*

Summary

Within the Critical Patch Update for July 2021 addressing hundreds of vulnerabilities across multiple products [1], Oracle released information about **critical vulnerabilities affecting WebLogic Server**.

Technical Details

Oracle WebLogic Server is an application server used as a platform for developing, deploying and running enterprise Java-based applications. In the Critical Patch Update for July 2021, there are fixes for several WebLogic Server flaws, four of which have been assigned a CVSS score of 9.8 out of 10:

- CVE-2019-2729, a critical deserialization vulnerability via XMLDecoder in Oracle WebLogic Server Web Services that is remotely exploitable without authentication [2],
- CVE-2021-2394, easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server [3],
- CVE-2021-2397, similar to CVE-2021-2394 [4],
- CVE-2021-2382, similar to CVE-2021-2394 [5].

Affected Products

The vulnerability exists in Oracle WebLogic Server, specific versions mentioned in [2], [3], [4], [5].

Recommendations

It is recommended to apply the necessary patches from the Critical Patch Update for July 2021 [1] as soon as possible.

CERT-EU recommends updating the vulnerable application as soon as possible.

References

[1] https://www.oracle.com/security-alerts/cpujul2021.html

[2] https://www.oracle.com/security-alerts/alert-cve-2019-2729.html

[3] https://nvd.nist.gov/vuln/detail/CVE-2021-2394

[4] https://nvd.nist.gov/vuln/detail/CVE-2021-2397

[5] https://nvd.nist.gov/vuln/detail/CVE-2021-2397