Security Advisory 2020-026

Critical Oracle WebLogic Server Vulnerability Exploited

May 12, 2020 — v1.0

TLP:WHITE

History:

- *12/05/2020 — v1.0 – Initial publication*

Summary

In April, within the monthly Critical Patch Update Advisory addressing hundreds of vulnerabilities [1], Oracle released an update about a **critical vulnerability affecting WebLogic Server**. This vulnerability allows **remote attackers** to **execute arbitrary code** on affected installations of Oracle WebLogic. Authentication is not required to exploit this vulnerability. This bug, assigned with CVE-2020-2883, is now being reported by Oracle as being **actively exploited in the wild** [5].

Technical Details

The vulnerability was initially assigned with CVE-2020-2555 and patched by Oracle in January 2020 [2]. On 15th of January 2020, CERT-EU has issued **Security Advisory 2020-004** that addressed, among others, CVE-2020-2555 as well [3].

However, according to Zero-Day Initiative, the patch made available in January by Oracle **can by bypassed** [4]. The specific flaw exists within the Oracle Coherence library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to **execute code** in the context of the **service account**. This by-pass has been patched in the April by Oracle as CVE-2020-2883. This vulnerability is now reported to be under active exploitation [5].

Affected Products

The vulnerability exists in Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 [1].

Recommendations

It is recommended to apply the necessary patches from the April Oracle Critical Patch Update [1] as soon as possible.

References

[1] https://www.oracle.com/security-alerts/cpuapr2020.html

[2] https://www.oracle.com/security-alerts/cpujan2020.html

[3] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-004.pdf

[4] https://www.zerodayinitiative.com/blog/2020/5/8/details-on-the-oracle-weblogic-vulnerability-being-exploited-in-the-wild

[5] https://blogs.oracle.com/security/apply-april-2020-cpu