CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-054

Critical Vulnerability in Oracle WebLogic Server

November 3, 2020 — v1.0

TLP:WHITE

History:

- *3/11/2020 — v1.0 – Initial publication*

Summary

On the 1st of November 2020, Oracle released an out-of-band patch to address a critical vulnerability (**CVSS score 9.8**) that has been assigned **CVE-2020-14750** [1]. According to Oracle, this bug is linked to the vulnerability **CVE-2020-14882** [2]. However, Oracle did not provide any information about the relation between both of the security flaws. The CVE-2020-14750 vulnerability could allow a non-authenticated attacker to remotely execute arbitrary code on the server.

Technical Details

Oracle did not provide any technical information about the vulnerability. However, some sources believe the CVE-2020-14750 patch addresses a bypass of the CVE-2020-14882 patch, released some days ago [3].

As a reminder, **CVE-2020-14882** vulnerability involves different weaknesses in the way the server handles user-supplied requests. An attacker could send a simple HTTP GET request to exploit the vulnerability, execute code and get full control on the server [4].

Affected Products

The vulnerability exists in Oracle WebLogic Server, versions [1]:

- 10.3.6.0.0,
- 12.1.3.0.0,
- 12.2.1.3.0,
- 12.2.1.4.0,
- 14.1.1.0.0.

Recommendations

It is recommended to apply the necessary patches from the October Oracle Critical Patch Update [1] as soon as possible and to look for any indicator of compromised on your network, beginning with firewall logs.

References

[1] https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-053.pdf

[3] https://www.bleepingcomputer.com/news/security/oracle-issues-emergency-patch-for-critical-weblogic-server-flaw/

[4] https://testbnull.medium.com/weblogic-rce-by-only-one-get-request-cve-2020-14882-analysis-6e4b09981dbf