CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-053

Critical Vulnerability in Oracle WebLogic Server

October 30, 2020 — v1.0

TLP:WHITE

History:

- *30/10/2020 — v1.0 – Initial publication*

Summary

In October, 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 may allow **unauthenticated attackers** with network access via HTTP to achieve **total compromise and takeover** of vulnerable Oracle WebLogic Servers [2]. This bug has been assigned **CVE-2020-14882** and has a **CVSS score of 9.8** and is now being reported as being **exploited in the wild** [3].

Technical Details

The bug 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].

To address this vulnerability, a patch has been released by Oracle in October 2020. **This vulnerability is now reported to be under active exploitation** [5].

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.

Detection of Exploitation

The following strings in GET requests could be an indication of successful exploitation [5]:

- `/console/images/%252E%252E%252Fconsole.portal`
- `/console/css/%252E%252E%252Fconsole.portal`

References

[1] https://www.oracle.com/security-alerts/cpuoct2020.html

[2] https://www.helpnetsecurity.com/2020/10/29/cve-2020-14882/

[3] https://www.bleepingcomputer.com/news/security/critical-oracle-weblogic-flaw-actively-targeted-in-attacks/

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

[5] https://isc.sans.edu/diary/rss/26734