Alert – A Vulnerability in Oracle WebLogic Could Allow for Remote Code Execution

Description/Overview:

A highly critical zero-day vulnerability has been discovered in the **Oracle WebLogic server application** that some attackers might have already started exploiting in the wild and that could also allow for remote code execution. Oracle WebLogic is a scalable, Java-based multi-tier enterprise application server that allows businesses to quickly deploy new products and services on the cloud. It's popular across both, cloud environment and conventional environments and it's used for building and hosting Java-EE applications.
Successful exploitation of this vulnerability could result in remote code/commands execution within the context of the application (affected servers) just by sending a specially crafted HTTP request—without requiring any authorization. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Vulnerable or affected versions:

All versions of Oracle WebLogic with WLS9_ASYNC and WLS-WSAT components enabled, namely:

- WebLogic 10.X
- WebLogic 12.1.3

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **HIGH**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **HIGH**

Solution:

Rw-CSIRT is strongly recommending **Server administrators** (managed environments) to:

- As a temporary workaround, consider disabling the WLS9_ASYNC and WLS-WSAT components until a security patch is available.
- When available, apply appropriate updates provided by Oracle to affected systems immediately after appropriate testing.
- Apply the Principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

So, until the company releases an update to patch the vulnerability, server administrators are highly recommended to prevent their systems from exploitation by changing either of the two following settings:

- Finding and deleting wls9_async_response.war, wls-wsat.war and restarting the Weblogic service, or
- Preventing access to the /_async/* and /wls-wsat/* URL paths via access policy control.

Affected users should: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

Vulnerability Details:
https://www.tenable.com/blog/oracle-weblogic-affected-by-unauthenticated-remote-code-execution-vulnerability-cve-2019-2725

References:
https://www.oracle.com/middleware/weblogic/
https://thehackernews.com/2019/04/oracle-weblogic-hacking.html
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.