Vulnerability Alert

Alert No: AVA190426 **Date: 26-Apr-19 13:04 PM**

Classification	**The Alert : Public Circulation Permitted**

High Critical: Oracle WebLogic Server Zero-Day Flaw

Overview	**An unpatched zero-day vulnerability in Oracle's WebLogic has been identified as being exploited in the wild.**
Description / Impact	It has come to light, though a report released by a cybersecurity research organization, that Oracle WebLogic server has an unpatched vulnerability that is suspected of currently being exploited by malicious attackers. It is reported that the application contains a deserialization remote code execution vulnerability that affects all versions of the software. This vulnerability can be exploited if the "wls9_async_response.war" and the wls.wsat.war" components are enabled by using a specially crafted HTTP request, without requiring authorization. Not officially acknowledged by the vendor.
Risk Reduction Recommendation	An official patch has not been released by the vendor at this time. The following however have been reported as possible work arounds until the issue is resolved. One of the following: • Remove "wls9_async_response.war" and " wls-wsat.war" and once done, restart the Weblogic service. • Through perimeter device and/or other security devices, define access control policies to deny access to "/_async/*" and "/wls-wsat/*" URL paths.
Additional Information	**Visit the links below and follow the instructions given by respective vendors.** • https://medium.com/@knownseczoomeye/knownsec-404-team-oracle-weblogic-deserialization-rce-vulnerability-0day-alert-90dd9a79ae93 • https://thehackernews.com/2019/04/oracle-weblogic-hacking.html
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.