Un equipo de investigadores de seguridad cibernética publicó hoy una advertencia posterior de una vulnerabilidad de día cero sin parches muy crítica en la aplicación del servidor Oracle WebLogic que algunos atacantes ya podrían haber comenzado a explotar.

Oracle WebLogic es un servidor de aplicaciones empresariales multinivel escalable y basado en Java que permite a las empresas implementar rápidamente nuevos productos y servicios en la nube. Es popular en entornos de nube como en entornos convencionales.

Según el reporte, la aplicación Oracle WebLogic contiene una vulnerabilidad de ejecución remota de código de deserialización crítica que afecta a todas las versiones del software, que se puede activar si los componentes *«wls9_async_response.war»* y *«wls-wsat.war»* están habilitados.

La vulnerabilidad, detectada por los investigadores de KnownSec 404, permite a los hackers ejecutar comandos arbitrarios de forma remota en los servidores afectados con solo enviar una solicitud HTTP especialmente diseñada, sin requerir ninguna autorización.

> *«Dado que el paquete WAR tiene un defecto en la deserialización de la información de entrada, el atacante puede obtener la autorización del servidor de destino mediante el envío de una solicitud HTTP maliciosa cuidadosamente creada, y ejecutar el comando de forma remota sin autorización»*, explica la Chinese National Information Security Vulnerability Sharing Platform (CNVD).

Los investigadores también compartieron detalles acerca de la vulnerabilidad 0Day, rastreados como CNVD-C-2019-48814, con el equipo de Oracle, pero la compañía no ha lanzado un parche. Las versiones de Oracle WebLogic afectadas son las siguientes:

- WebLogic 10.X
- wbLogic 12.1.3

De acuerdo con el motor de búsqueda del ciberespacio de ZoomEye, más de 36,000

servidores WebLogic son de acceso público en Internet, aunque no se sabe cuántos de ellos tienen habilitados los componentes vulnerables.

Un número máximo de servidores Oracle WebLogic se implementa en Estados Unidos y China, con un número menor en Irán, Alemania, India, etc.

Debido a que Oracle publica actualizaciones de seguridad cada tres meses y ya había lanzado una actualización de parche crítico este mes, es poco probable que este problema se solucione pronto, a menos que la compañía decida implementar una actualización de seguridad fuera de banda.

Por lo tanto, hasta que la compañía publique una actualización para corregir la vulnerabilidad, se recomienda encarecidamente a los administradores de servidores que eviten que sus sistemas se aprovechen al cambiar una de las siguientes configuraciones:

- Buscando y eliminando wls9_async_response.war, wls-wsat.war y reiniciando el servidor WebLogic.
- Evitar el acceso a las rutas URL / _async / * y / wls-wsat / * mediante el control de la política de acceso.

Ya que los servidores de Oracle WebLogic son un blanco frecuente de los hackers, no habrá ninguna sorpresa si los atacantes ya comenzaron a explotar esta vulnerabilidad.