Infórmate

Nueva Falla Crítica De Oracle Weblogic Bajo Ataque Activo

Oracle ha lanzado una actualización de software de emergencia fuera de banda para parchear una vulnerabilidad crítica recientemente descubierta en el servidor WebLogic.

Según Oracle, la vulnerabilidad, que puede identificarse como CVE-2019-2729 y tiene un puntaje CVSS de **9.8** sobre **10**, ya está siendo explotada en la naturaleza por un grupo de atacantes no identificado.

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

La vulnerabilidad informada es un problema de deserialización a través de XMLDecoder en los servicios web del servidor Oracle WebLogic que podría permitir a atacantes remotos no autorizados ejecutar código arbitrario en los servidores de destino y tomar el control sobre ellos.

"Esta vulnerabilidad de ejecución remota de código se puede explotar de forma remota sin autenticación, es decir, se puede explotar a través de una red sin la necesidad de un nombre de usuario y contraseña", dijo el aviso.

En una nota separada, la compañía también reveló que la falla está relacionada con una vulnerabilidad de deserialización previamente conocida (CVE-2019-2725) en Oracle WebLogic Server que parchó en abril de este año.

La falla de RCE previamente parcheada en Oracle WebLogic también fue explotada por los atacantes como un día cero, es decir, para distribuir el ransomware Sodinokibi y el malware de minería de criptomonedas.

Informada de forma independiente por un grupo separado de individuos y organizaciones, la nueva vulnerabilidad afecta a Oracle WebLogic Server versiones 10.3.6.0.0, 12.1.3.0.0 y 12.2.1.3.0.

Debido a la gravedad de esta vulnerabilidad, la compañía ha recomendado a los usuarios afectados y a las compañías que instalen actualizaciones de seguridad disponibles lo antes posible.

Fuente: https://thehackernews.com/2019/06/dells-supportassist-hacking.html