Oracle lanzó este martes su actualización de parche crítico trimestral para julio de 2021, con 342 correcciones que abarcan múltiples productos, algunos de los cuales podrían ser explotados por un atacante remoto para tomar el control de un sistema infectado.

El principal de ellos es CVE-2019-2729, una vulnerabilidad de deserialización crítica a través de XMLDecoder en Oracle WebLogic Server Web Services, que puede ser explotada de forma remota sin autenticación.

Cabe mencionar que la vulnerabilidad se abordó originalmente como parte de una actualización de seguridad fuera de banda en junio de 2019.

Oracle WebLogic Server es un servidor de aplicaciones que funciona como una plataforma para desarrollar, implementar y ejecutar aplicaciones empresariales basadas en Java.

La vulnerabilidad, que tiene una calificación de 9.8 de un máximo de 10 en escala CVSS, afecta a las versiones 11.1.2.4 y 11.2.5.0 de WebLogic Server, y existe dentro de la tecnología de infraestructura Oracle Hyperion.

También se han corregido en WebLogic Server otras seis vulnerabilidades, a tres de las cuales se les asignó una puntuación CVSS de 9.8 sobre 10:

- CVE-2021-2394 (puntuación CVSS de 9.8)
- CVE-2021-2397 (puntuación CVSS de 9.8)
- CVE-2021-2382 (puntuación CVSS de 9.8)
- CVE-2021-2378 (puntuación CVSS de 7.5)
- CVE-2021-2376 (puntuación CVSS de 7.5)
- CVE-2021-2403 (puntuación CVSS de 5.3)

Esta no es la primera vez que se descubren problemas críticos en WebLogic Server. A inicios de este año, Oracle envió el parche de abril de 2021 con correcciones para dos errores (CVE-2021-2125 y CVE-2021-2136), entre otros que podrían abusarse para ejecutar código arbitrario.

Se recomienda a los clientes de Oracle que actúen rápidamente para aplicar las actualizaciones y proteger los sistemas contra una posible explotación.