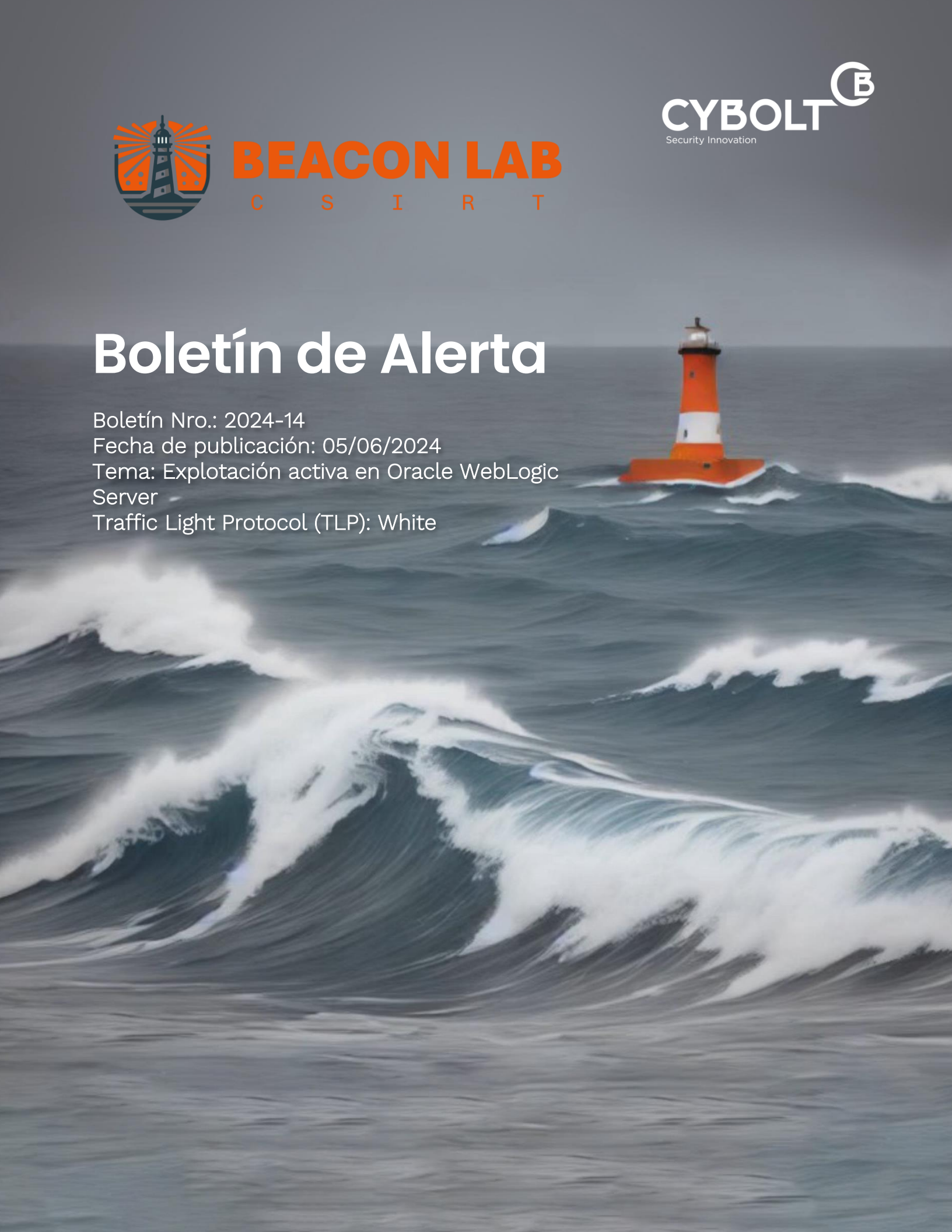
BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-14
Fecha de publicación: 05/06/2024
Tema: Explotación activa en Oracle WebLogic Server
Traffic Light Protocol (TLP): White



Producto(s) afectado:

Oracle WebLogic Server, componente de la suite Oracle Fusion Middleware.

- Versiones afectadas:
  - 10.3.6.0
  - 12.1.3.0
  - 12.2.1.0
  - 12.2.1.1
  - 12.2.1.2

Descripción

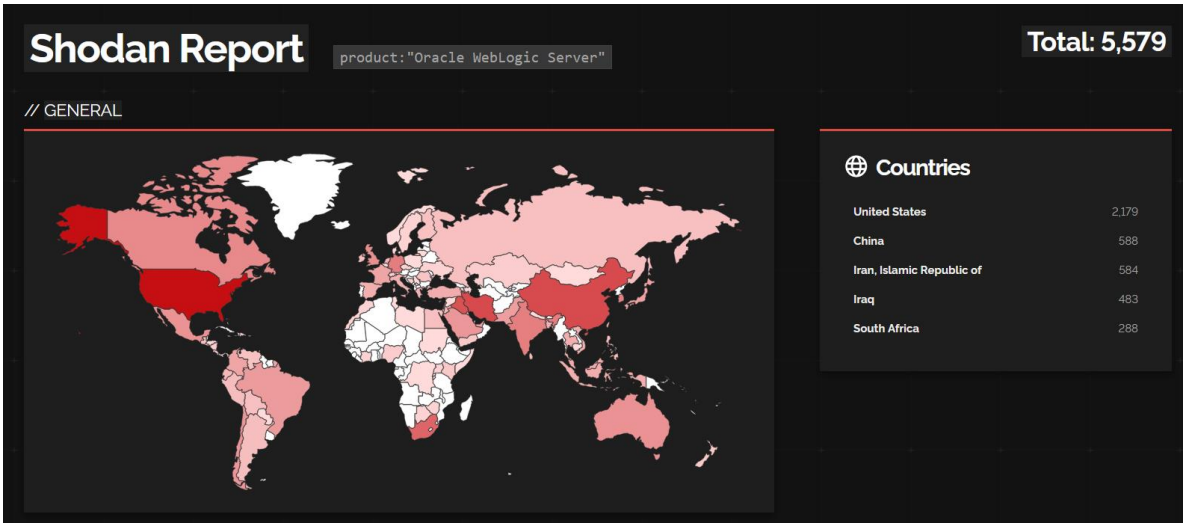
Recientemente se ha reportado un aumento de la explotación activa de la vulnerabilidad CVE-2017-3506 de Oracle WebLogic por parte de grupos criminales. Esta vulnerabilidad, con una puntuación de severidad de 7.4, reside en un componente de la suite de Oracle Fusion Middleware, al explotar la vulnerabilidad mencionada, permite a los atacantes no autenticados la inyección de comandos a nivel de sistema operativo, a través de la modificación de las peticiones de HTTP, aprovechándose de la funcionalidad de procesamiento de XML del servidor.

Además, es importante mencionar que cualquier explotación exitosa, puede llevar a la creación, modificación, o eliminación de datos existentes en nuestro Oracle WebLogic, incluso se podría el ataque, podría expandirse por la red.

Cabe recalcar que esta vulnerabilidad fue descubierta en el año 2017, sin embargo, actualmente se está avistando una explotación concurrente de esta vulnerabilidad, por el grupo 8220 Gang, un grupo chino enfocado en el cryptojacking (explotación de activos para la minería de criptomonedas sin consentimiento) puede deberse a que muchos de estos aplicativos no han sido actualizados y quizás al uso de algún exploit de prueba de concepto de esta vulnerabilidad. La Cybersecurity and Infrastructure Security Agency de EEUU (CISA) la ha añadido a su base de datos de KEV (Known Exploited Vulnerabilities).

Oracle WebLogic es un producto muy popular, con caso 5.600 servidores expuestos a Internet en el mundo. En Mexico existen múltiples servidores expuestos a Internet, y también como parte de aplicativos internos, que, aunque podrían no estar expuestos de manera directa a Internet, podrían ser aprovechado como parte de la

estrategia de movimiento lateral entre sistemas por parte de un atacante que ya hubiera ganado acceso a la red.



Impacto

Un actor malintencionado que pueda alcanzar remotamente nuestro aplicativo Oracle WebLogic Server, podría modificar nuestros datos locales, y además, podría extender el ataque a toda la red interna, así teniendo un gran impacto en la infraestructura.

Solución

Actualizar el software Oracle Weblogic a las últimas versiones que corrigen esta vulnerabilidad.

Información adicional:

- Zero-Day Protection Against Oracle Weblogic Server OS Command | Waratek
- NVD - CVE-2017-3506 (nist.gov)
- Oracle WebLogic Server OS Command Injection Flaw Under Active Attack (thehackernews.com)
- Known Exploited Vulnerabilities Catalog | CISA

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com