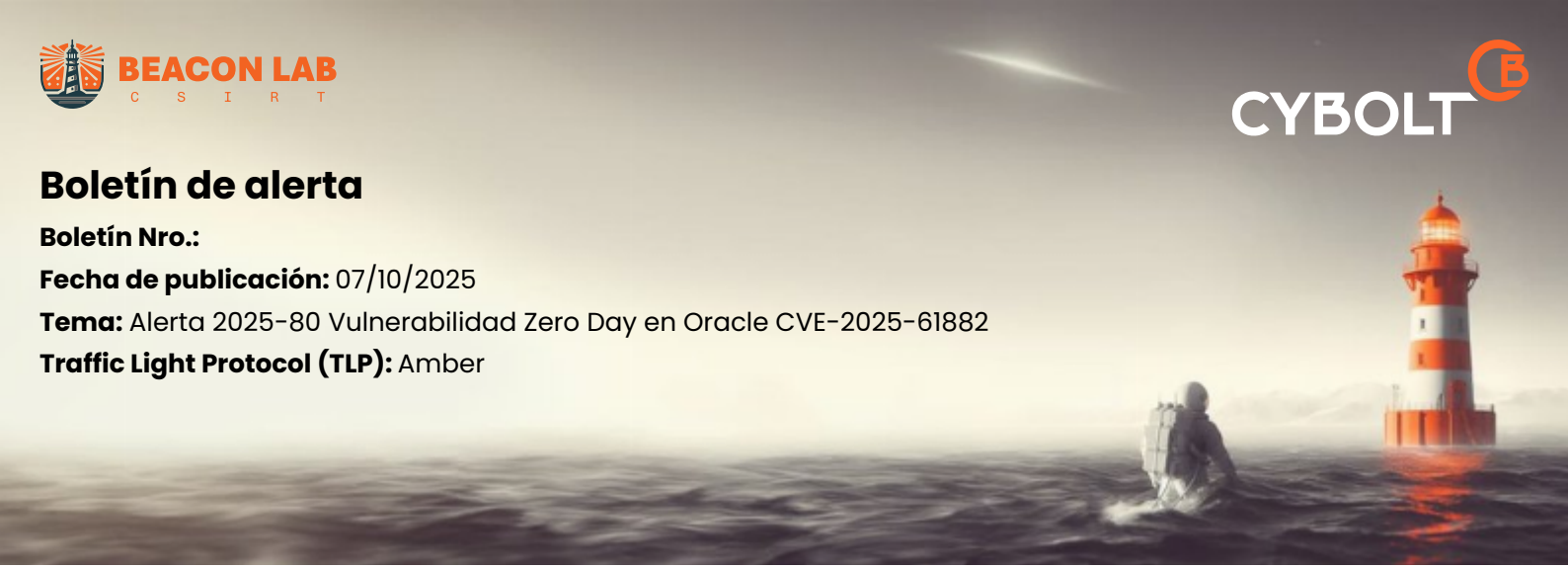

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 07/10/2025
Tema: Alerta 2025-80 Vulnerabilidad Zero Day en Oracle CVE-2025-61882
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Oracle E-Business Suite, versions 12.2.3-12.2.14

Descripción

Recientemente se ha reportado una nueva vulnerabilidad de Día Cero (Zero Day) en productos Oracle E-Business Suite, la misma ha sido identificada como CVE-2025-61882 con un puntaje CVSS de 9.8 de tipo RCE, la cual permite a atacantes remotos no autenticados comprometer el componente de Procesamiento Concurrente de Oracle a través de peticiones HTTP especialmente modificadas y esto le permitiría al atacante obtener control total sobre los sistemas afectados. Se reporta que está siendo explotada activamente en la última campaña de robo de datos vinculada al grupo Cl0p.

La vulnerabilidad afecta al componente BI Publisher Integration de Oracle Concurrent Processing y permite **RCE** remoto sin autenticación. Explotarla es sencillo, debido a la ausencia de controles previos, y ya circulan exploits y PoC públicos (basados en Python) filtrados por grupos como Scattered Lapsus$ Hunters. El exploit permite tanto ejecutar comandos arbitrarios como establecer reverse shells hacia servidores controlados por el atacante.

El impacto es elevado, la facilidad de explotación y la existencia de PoCs públicos incrementan el riesgo de ataques masivos. Ya se han reportado incidentes de **robo de datos** y extorsión en compañías de todo el mundo, con amenazas de publicar información sensible si no se paga rescate. La situación podría escalar si otros actores adoptan el exploit en nuevos ataques.

Solución:

Oracle ha publicado un **parche de emergencia** que debe aplicarse tras instalar la Critical Patch Update de octubre 2023.

- https://support.oracle.com/rs?type=doc&id=3106344.1

Es vital actualizar inmediatamente y revisar los indicadores de compromiso (IPs, comandos, archivos de exploit) difundidos por Oracle. Se recomienda auditar el acceso de red a estos sistemas y reforzar la monitorización proactiva de logs y alertas en entornos potencialmente afectados.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2025-61882
- https://labs.watchtowr.com/well-well-well-its-another-day-oracle-e-business-suite-pre-auth-rce-chain-cve-2025-61882well-well-well-its-another-day-oracle-e-business-suite-pre-auth-rce-chain-cve-2025-61882/
- https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
- https://www.bleepingcomputer.com/news/security/oracle-patches-ebs-zero-day-exploited-in-clop-data-theft-attacks/
- https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882/