Boletín informativo vulnerabilidad Oracle E-Business Suite

CSIRTSALUD-AV-20251021-07

TLP: CLEAR

Incidente ID:	0007
Fecha del reporte:	21/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Oracle E-Business Suite
Herramienta de detección	N/A
Activo involucrado:	Módulo Oracle Configurator
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad de explotación remota identificada como CVE-2025-61884 que afecta el módulo Oracle Configurator dentro de Oracle E-Business Suite, en particular el componente de la interfaz de usuario Runtime.

Boletín informativo vulnerabilidad Oracle E-Business Suite

CSIRTSALUD-AV-20251021-07 **TLP: CLEAR**

Descripción:

La vulnerabilidad de Oracle E-Business Suite identificada públicamente como CVE-2025-61884 afecta la interfaz de usuario Runtime del producto Oracle Configurator de Oracle E-Business Suite (EBS).
Al igual que CVE-2025-61882 antes que esta, afecta oficialmente a las versiones ESB 12.2.3 a 12.2.14.
Según la entrada de la base de datos nacional de vulnerabilidades del NIST para CVE-2025-61884, se trata de una vulnerabilidad fácilmente explotable que permite a un atacante no autenticado con acceso a la red a través de HTTP comprometer Oracle Configurator. Los ataques exitosos de esta vulnerabilidad pueden resultar en el acceso no autorizado a datos críticos o el acceso completo a todos los datos accesibles de Oracle Configurator.
Rob Duhart, CIS de Oracle Security, dice que la vulnerabilidad “puede permitir el acceso a recursos sensibles” y “afecta algunas implementaciones de Oracle E-Business Suite”.

Productos afectados:

- ESB 12.2.3
- ESB 12.2.4
- ESB 12.2.5
- ESB 12.2.6
- ESB 12.2.7
- ESB 12.2.8
- ESB 12.2.9
- ESB 12.2.10
- ESB 12.2.11
- ESB 12.2.12

- ESB 12.2.13
- ESB 12.2.14

Todas estas versiones comparten el mismo módulo afectado el de Oracle Configurator (Runtime UI Component)

Como se podría explotar esta vulnerabilidad

Un atacante con acceso de red hacia la interfaz web vulnerable envía peticiones HTTP especialmente formadas al componente Runtime UI del Oracle Configurator. Debido a controles de autorización/validaciones insuficientes, esas peticiones pueden devolver o permitir acceso a recursos/datos que deberían estar protegidos. Esa es la razón por la que la vulnerabilidad es remota y sin necesidad de autenticación.

Sectores afectados

Gobierno, Salud, financiero, energía, TIC, educación, transporte, comercio, industria, Recursos humanos, sanidad, telecomunicaciones y turismo.

Matriz de Riesgo

Ítem	Detalle
CVE	CVE-2025-61884
Vector	CVSS:3.1
Base score	7.5
Protocolo	HTTP
Vector de ataque	Red

Ítem	Detalle
Explotación remota sin autenticación	Si
Complejidad del ataque	Bajo
Requiere privilegios	Ninguno
Interacción con el usuario	Ninguno
Ámbito	Sin cambio
Confidencialidad	Alto
Integridad	Ninguno
Disponibilidad	Ninguno

Recomendaciones de mitigación:

- Aplicar el parche de Oracle inmediatamente: Oracle publicó un Security Alert y parches de emergencia. Prioriza servidores 12.2.3–12.2.14. Verifica la nota oficial y el MOS correspondiente.

  Enlace de descarga de parches
  - o https://www.oracle.com/security-alerts/?utm_source

Si no se puede aplicar el parche de manera inmediata se recomienda seguir las siguientes recomendaciones

- Bloquear el acceso HTTP(S) al EBS desde Internet (usar ACLs/Firewall) — deja acceso sólo desde red corporativa/vpn/hosts de confianza.
- Desplegar reglas WAF para bloquear tráfico anómalo hacia las páginas/servicios EBS (bloqueo genérico de solicitudes sospechosas).
- imitar salida/entradas salientes desde el servidor EBS (evitar que un intruso exfiltre datos).

- revisar logs web (requests HTTP anómalos), logs de aplicaciones EBS, creación/modificación de plantillas o jobs, cuentas nuevas, ejecuciones de procesos concurrentes inesperadas y conexiones salientes inusuales.
- inventariar todas las instancias EBS (12.2.3–12.2.14) en la Entidad y aplicar parches o mitigaciones de forma priorizada por criticidad / exposición y se recomienda ejecutar un escaneo de vulnerabilidades a los equipos internos y externos para confirmar estado.

Fuentes:

- https://www.helpnetsecurity.com/2025/10/12/another-remotely-exploitable-oracle-ebs-vulnerability-requires-your-attention-cve-2025-61884/
- https://www.oracle.com/security-alerts/alert-cve-2025-61884.html?utm_source
- https://thehackernews.com/2025/10/new-oracle-e-business-suite-bug-could.html?utm_source

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.