Boletín informativo vulnerabilidad Marketing de Oracle E-Business Suite

CSIRTSALUD-AV-20251030-11 **TLP: CLEAR**

Incidente ID:	0011
Fecha del reporte:	30/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Oracle E-Business Suite
Herramienta de detección	N/A
Activo involucrado:	Componente Marketing de su E-Business Suite
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre las dos vulnerabilidades críticas que afectan a la administración del componente Marketing de Oracle E-Business Suite, permitiendo a atacantes remotos sin autenticación tomar control total. Las vulnerabilidades fueron nombradas con los CVE-2025-53072 y CVE-2025-62481 las cuales presentan puntaje de CVSS 9.8 debido a su impacto elevado en confidencialidad, integridad y disponibilidad, explotándose mediante solicitudes HTTP sin interacción del usuario.

Boletín informativo vulnerabilidad Marketing de Oracle E-Business Suite

CSIRTSALUD-AV-20251030-11 **TLP: CLEAR**

Descripción:

Oracle ha divulgado dos vulnerabilidades críticas, CVE-2025-53072 y CVE-2025-62481, en el componente de Administración de Marketing de su E-Business Suite. Estas vulnerabilidades permiten a atacantes no autenticados obtener el control total del módulo de Marketing de Oracle mediante una única solicitud HTTP. Con una puntuación CVSS de 9.8, estas vulnerabilidades se encuentran entre las amenazas más graves divulgadas este año, lo que supone un riesgo significativo para las organizaciones que utilizan la suite de Oracle para la gestión de relaciones con los clientes y la automatización del marketing.

Las vulnerabilidades se originan en deficiencias en el procesamiento de solicitudes HTTP por parte del componente de Administración de Marketing. Un atacante con acceso a la red puede aprovechar estas fallas sin necesidad de privilegios especiales ni interacción del usuario. Si la explotación tiene éxito, el sistema Oracle Marketing queda totalmente comprometido, lo que afecta la confidencialidad, la integridad y la disponibilidad.

CVE ID	Componente	Vector de ataque	CVSS 3.1	Impacto en C/I/A	Versiones afectadas
CVE-2025-53072	Marketing Administration	HTTP (Red)	9.8	Alta/Alta/Alta	12.2.3 – 12.2.14
CVE-2025-62481	Marketing Administration	HTTP (Red)	9.8	Alta/Alta/Alta	12.2.3 – 12.2.14

Boletín informativo vulnerabilidad Marketing de Oracle E-Business Suite

CSIRTSALUD-AV-20251030-11 **TLP: CLEAR**

Productos afectados:

- Producto Principal: Oracle E-Business Suite
- Componente Específico: Oracle Marketing (Marketing Administration)
- Versiones Afectadas: 12.2.3 hasta 12.2.14

Como se podría explotar esta vulnerabilidad

Estas vulnerabilidades son especialmente peligrosas porque pueden ser explotadas de forma remota y no requieren autenticación.

- Vector de Ataque: Red
- Autenticación: No requerida
- Interacción del Usuario: No requerida

Un atacante remoto puede enviar una solicitud HTTP diseñada específicamente al componente vulnerable. Debido a que el sistema no valida adecuadamente esta entrada, el atacante puede comprometer el sistema sin necesidad de credenciales de usuario ni de que un usuario legítimo realice ninguna acción, lo que permite que el sistema Oracle Marketing queda totalmente comprometido, lo que afecta la confidencialidad, la integridad y la disponibilidad.

Sectores afectados

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

Boletín informativo vulnerabilidad Marketing de Oracle E-Business Suite

CSIRTSALUD-AV-20251030-11 **TLP: CLEAR**

Matriz de Riesgo

Ítem	Detalle	
CVE	CVE-2025-53072	CVE-2025-62481
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Base score	9.8 (Crítico)	9.8 (Crítico)
Protocolo	HTTP	HTTP
Vector de ataque	Red	Red
Explotación remota sin autenticación	Sí	Sí
Complejidad del ataque	Baja	Baja
Requiere privilegios	Ninguno	Ninguno
Interacción con el usuario	Ninguna	Ninguna
Ámbito	Sin cambios	Sin cambios
Confidencialidad	Alta	Alta
Integridad	Alta	Alta
Disponibilidad	Alta	Alta

Recomendaciones de mitigación:

Se insta a las organizaciones que utilicen las versiones afectadas de Oracle E-Business Suite a tomar medidas inmediatas.

- Solución Primaria (Parche): Oracle ha abordado estas vulnerabilidades en su actualización de parches críticos más reciente. La solución es aplicar el Oracle Critical Patch Update (CPU) de octubre de 2025.
- Mitigación: Si no es posible aplicar el parche de inmediato, se recomienda restringir el acceso de red (especialmente el acceso HTTP) al componente de Oracle Marketing solo a usuarios y sistemas de confianza, para reducir la superficie de ataque.
- Aísle el componente de Administración de Marketing de las redes públicas para limitar su exposición. Esto puede ayudar a prevenir el acceso no autorizado de atacantes externos.
- Supervise continuamente el tráfico de red y los registros de aplicaciones de Administración de Marketing para detectar patrones inusuales o intentos de acceso no autorizados.
- Configurar firewalls de aplicaciones web para detectar anomalías HTTP y la monitorización del tráfico inusual de administración de marketing.

Fuentes:

- https://www.oracle.com/security-alerts/cpuoct2025.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/oracle-vulnerabilidades-criticas-en-marketing-de-e-business-suite/
- https://www.tenable.com/plugins/nessus/271365
- https://kudelskisecurity.com/research/critical-vulnerabilities-in-oracle-e-business-suite-marketing-administration
- https://cyble.com/blog/cyble-weekly-700-vulnerabilities-46-critical-pocs/

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.