Nro. Alerta:	AL-2025-009	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	01-mar-2025	**Vulnerabilidad en productos Adobe y Oracle**	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Inyección de Código

Nivel de riesgo: Alto

II. ALERTA

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha añadido dos vulnerabilidades críticas a su Catálogo de Vulnerabilidades Explotadas Conocidas "KEV" (de sus siglas en inglés), afectando a dos productos ampliamente utilizados: Adobe ColdFusion y Oracle Agile Product Lifecycle Management (PLM). Estas fallas, identificadas como CVE-2017-3066 y CVE-2024-20953, ya están siendo aprovechadas por ciberdelincuentes.

Figura 1.- *Ilustración asociada a Adobe y Oracle* ***Fuente: DRA***

III. INTRODUCCIÓN

Las vulnerabilidades mencionadas se encuentran rastreadas mediante los identificadores CVE2017-3066 y CVE-2024-20953 respectivamente y son vulnerabilidades que afectan a las series de fábrica de los productos, que de ser explotadas, podrían conducir a ejecución remota de código.

Ambas vulnerabilidades están relacionadas con fallas serie de productos, un problema recurrente en ciberseguridad. Cuando una aplicación procesa datos no confiables sin las medidas adecuadas, los atacantes pueden inyectar código malicioso para tomar el control del sistema, escalar privilegios o ejecutar comandos peligrosos. Esto las convierte en una puerta de entrada ideal para ataques como robo de información, ransomware y accesos no autorizados.

IV. VECTOR DE ATAQUE.

Las vulnerabilidades en cuestión se enumeran a continuación:

- **CVE-2017-3066** (puntuación CVSS: 9,8): vulnerabilidad de deserialización que afecta a Adobe ColdFusion en la biblioteca Apache BlazeDS y que permite la ejecución de código arbitrario. (Corregido en abril de 2017).
- **CVE-2024-20953** (puntuación CVSS: 8,8): vulnerabilidad de deserialización que afecta a Oracle Agile PLM y que permite que un atacante con pocos privilegios y acceso a la red a través de HTTP ponga en peligro el sistema. (Corregido en enero de 2024)

Para mitigar los riesgos que plantean los posibles ataques que utilicen estas fallas como arma, se recomienda que los usuarios tomen medidas para aplicar las actualizaciones necesarias.

V. IMPACTO

Las vulnerabilidades en cuestión producen los siguientes impactos:

CVE-2017-3066:

Esta vulnerabilidad fue reportada por primera vez en 2017 y afecta a **Adobe ColdFusion**, específicamente a la biblioteca **Apache BlazeDS** que usa este software.

El problema es que ColdFusion no valida correctamente los datos cuando los deserializa, lo que abre la puerta a que los atacantes inyecten código malicioso. En otras palabras, si esta falla no se corrige, un hacker podría ejecutar comandos en el sistema afectado e incluso tomar el control total.

Las versiones vulnerables incluyen:

- **ColdFusion 2016** (Actualización 3 y anteriores).
- **ColdFusion 11** (Actualización 11 y anteriores).
- **ColdFusion 10** (Actualización 22 y anteriores).

Adobe lanzó parches en abril de 2017 para corregir el problema, pero el riesgo sigue presente en sistemas que no han aplicado las actualizaciones.

CVE-2024-20953:

Otra de las fallas críticas que CISA ha agregado es CVE-2024-20953, un problema grave en Oracle Agile Product Lifecycle Management (PLM). Esta vulnerabilidad afecta la versión 9.3.6 del software y permite a un atacante con acceso a la red (vía HTTP) aprovechar una falla de deserialización para ejecutar código malicioso.

En pocas palabras, si esta vulnerabilidad es explotada, un hacker podría tomar el control total del sistema afectado, lo que representa un riesgo enorme para las empresas que dependen de esta herramienta.

El nivel de peligrosidad es alto: tiene una calificación CVSS de 8.8, lo que significa que su impacto puede comprometer la confidencialidad, integridad y disponibilidad de los datos. Además, su facilidad de explotación la convierte en un objetivo atractivo para ciberdelincuentes.

VI. RECOMENDACIONES:

Si se utiliza ColdFusion, Adobe recomienda actualizar a las siguientes versiones para cerrar esta brecha de seguridad:

- **ColdFusion 2016** – Actualización 4.
- **ColdFusion 11** – Actualización 12.
- **ColdFusion 10** – Actualización 23.

Estas actualizaciones no solo solucionan la vulnerabilidad CVE-2017-3066, sino que también protegen contra otros problemas de seguridad, como CVE-2017-3008, una falla de XSS (Cross-Site Scripting).

Por otro lado, Si se utiliza Oracle Agile PLM, es crucial que se aplique el parche de seguridad que Oracle ha lanzado lo antes posible. No hacerlo podría dejar el sistema expuesto a ataques que podrían robar información crítica o interrumpir operaciones clave.

Aplicar los parches de seguridad, fortalecer la configuración de los sistemas y mantenerse informado son las mejores estrategias para evitar que los ciberdelincuentes exploten estas fallas.

VII. DESCARGO DE RESPONSABILIDAD.

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS.

- https://blog.ehcgroup.io/2025/02/25/14/00/58/18108/dos-fallos-de-seguridad-explotados-activamente-en-productos-de-adobe-y-oracle-detectados-por-cisa/cisa/ehacking/

- https://www.incibe.es/empresas/avisos/adobe-corrige-una-vulnerabilidad-critica-en-varios-de-sus-productos
- https://blog.tecnetone.com/cisa-a%C3%B1ade-vulnerabilidades-de-adobe-y-oracle-a-su-lista-cr%C3%ADtica
- https://www.incibe.es/empresas/avisos/multiples-vulnerabilidades-en-productos-adobe-actualiza