La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA, por sus siglas en inglés) añadió este lunes cinco vulnerabilidades a su Catálogo de Vulnerabilidades Conocidas y Explotadas (KEV), confirmando oficialmente que una falla recientemente revelada en Oracle E-Business Suite (EBS) ya ha sido utilizada en ataques reales.

La vulnerabilidad en cuestión es la CVE-2025-61884 (con una puntuación CVSS de 7.5), clasificada como una vulnerabilidad de tipo SSRF (falsificación de solicitudes del lado del servidor) en el componente Runtime de Oracle Configurator. Esta falla permitiría a actores maliciosos acceder sin autorización a información crítica.

CISA señaló que "esta vulnerabilidad puede ser explotada de forma remota sin necesidad de autenticación".

La CVE-2025-61884 es la segunda vulnerabilidad en Oracle EBS que ha sido aprovechada activamente, junto con la CVE-2025-61882 (puntuación CVSS de 9.8), un fallo crítico que podría permitir a atacantes no autenticados ejecutar código arbitrario en sistemas vulnerables.

A comienzos de este mes, el Grupo de Inteligencia de Amenazas de Google (GTIG) y Mandiant informaron que decenas de organizaciones podrían haber sido comprometidas tras la explotación de la CVE-2025-61882.

"Por ahora, no podemos atribuir las actividades de explotación observadas a un actor específico, aunque es probable que al menos parte de dicha actividad esté relacionada con actores involucrados en operaciones de extorsión vinculadas a la marca Cl0p," indicó Zander Work, ingeniero senior en seguridad del GTIG, en declaraciones la semana pasada.

Además, CISA incorporó otras cuatro vulnerabilidades al catálogo KEV:

- CVE-2025-33073 (CVSS 8.8): vulnerabilidad por control de acceso inadecuado en el cliente SMB de Microsoft Windows que podría derivar en una escalada de privilegios (corregida por Microsoft en junio de 2025).

- CVE-2025-2746 (CVSS 9.8): omisión de autenticación mediante rutas o canales alternativos en Kentico Xperience CMS, lo que permitiría a un atacante manipular objetos administrativos aprovechando el manejo incorrecto de contraseñas SHA1 vacías en la autenticación digest del servidor Staging Sync (solucionada por Kentico en marzo de 2025).
- CVE-2025-2747 (CVSS 9.8): otra falla de autenticación similar en Kentico Xperience CMS, esta vez relacionada con el tipo de servidor definido como «None», también corregida en marzo de 2025.
- CVE-2022-48503 (CVSS 8.8): validación incorrecta de índices de arreglos en el componente JavaScriptCore de Apple, que podría provocar ejecución de código arbitrario al procesar contenido web (Apple lo solucionó en julio de 2022).

Actualmente no se ha confirmado cómo están siendo explotadas estas cuatro vulnerabilidades adicionales, aunque investigadores de Synacktiv y watchTowr Labs compartieron información técnica sobre las CVE-2025-33073, CVE-2025-2746 y CVE-2025-2747.

Las agencias del Poder Ejecutivo Civil Federal (FCEB) tienen plazo hasta el 10 de noviembre de 2025 para mitigar estas vulnerabilidades y proteger sus redes ante amenazas activas.