Onapsis publicó un informe en el que revela los detalles técnicos sobre las vulnerabilidades que informó sobre E-Business Suite (EBS) de Oracle, un grupo integrado de aplicaciones diseñadas para automatizar CRM, ERP y SCM.

Oracle parchó las dos vulnerabilidades, denominadas *«BigDebIT»* y calificó un puntaje CVSS de 9.9 en una actualización crítica de parche (CPU) expulsado a inicios de enero. Pero la compañía dijo que aproximadamente el 50 por ciento de los clientes de Oracle EBS no han implementado los parches hasta ahora.

Las vulnerabilidades podrían ser explotadas por hackers para apuntar a herramientas de contabilidad como el Libro Mayor, en un intento por robar información confidencial y cometer fraude financiero.

Según los investigadores, *«un pirata informático no autenticado podría realizar una explotación automatizada en el módulo Libro Mayor, para extraer activos de una empresa y modificar tablas contables, sin dejar rastro».*

> *«La explotación exitosa de esta vulnerabilidad permitiría a un atacante robar datos financieros y causar demoras en cualquier informe financiero relacionado con los proceso de cumplimiento de la compañía»*, agregó.

Cabe mencionar que los vectores de ataque BigDebIT se suman a las vulnerabilidades PAYDAY ya informadas en EBS, descubiertas por Onapsis hace tres años, después de lo cual, Oracle lanzó una serie de parches a finales de abril de 2019.

Rastreados como CVE-2020-2586 y CVE-2020-2587, los defectos residen en el Sistema de Gestión de Recursos Humanos de Oracle (HRMS), en un componente llamado Driagramador de Jerarquía, que permite a los usuarios crear organizaciones y jerarquías de posición asociadas con una empresa. Juntos, pueden explotarse incluso si los clientes de EBS

implementaron parches lanzados en abril de 2019.

> *«La diferencia es que con estos parches, se confirma que incluso con los sistemas actualizados son vulnerables a estos ataques, y por lo tanto, deben priorizar la instalación de la CPU de enero»*, dijo la compañía en una nota de enero.

Una consecuencia de estos errores, si no se reparan, es la posibilidad de un fraude financiero y robo de información confidencial al atacar los sistemas de contabilidad de una empresa.

Oracle General Ledger es un software de procesamiento financiero automatizado que actúa como un depósito de información contable y se ofrece como parte de E-Business Suite, el conjunto integrado de aplicaciones de la compañía, que abarca la planificación de recursos empresariales (ERP), la gestión de la cadena de suministro (SCM), y gestión de relaciones con los clientes (CRM), que los usuarios pueden implementar en sus propios negocios.

General Ledger también se utiliza para generar informes financieros corporativos, así como para realizar auditorías para garantizar el cumplimiento de la Ley SOX de 2002.

Un atacante podría romper la confianza al explotar las fallas para modificar informes críticos en el libro mayor, incluida la manipulación fraudulenta de transacciones en los balances de una empresa.

> *«Por ejemplo, un atacante podría modificar el informe de saldo de prueba, que resume los saldos contables en un período determinado, prácticamente inadvertido, lo que resulta en resultados informados incorrectamente que fluyen sin ser detectados en los estados financieros. Esto podría terminar en resultados financieros archivados o informados de forma incorrecta»*, dijo Onapsis.

La importancia de parchear el software

Debido al riesgo financiero involucrado, se recomienda que las empresas que utilizan Oracle EBS realicen una evaluación inmediata para asegurarse de que no están expuestas a las vulnerabilidades y apliquen los parches para solucionarlos.

> *«Las organizaciones deben ser conscientes de que las herramientas GRC actuales y otros métodos de seguridad tradicionales (firewalls, controles de acceso, SoD y otros), serían ineficaces para prevenir este tipo de ataque en los sistemas vulnerables Oracle EBS»,* advirtieron los investigadores.
>
> *«Si las organizaciones tienen sistemas Oracle EBS orientados a Internet, la probabilidad de amenaza potencial se vería significativamente aumentada. Las organizaciones bajo ataque no se darán cuenta del ataque no conocerán el alcance del daño hasta que se encuentre evidencia de una auditoría interna o externa muy extensa»,* concluyeron.