Vulnerabilidad en Apache OFBiz

BCSC-Vulnerabilidad-Apache-OFBiz

TLP:WHITE

www.basquecybersecurity.eus

Marzo 2021

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

Se ha hecho pública una vulnerabilidad crítica que afecta a Apache OFBiz. Este software es un sistema de planificación de recursos empresariales (ERP) de código abierto que proporciona un conjunto de aplicaciones que integran y automatizan muchos de los procesos comerciales de una empresa. Estos procesos pueden ir desde la monitorización de la contabilidad, la gestión de las relaciones con los clientes, la administración de las operaciones de fabricación o la gestión de almacenes.

El fallo fue reportado mediante una colaboración entre investigadores de la compañía China QI ANXIN Technology Group y el ingeniero de ciberseguridad r00t4dm.

Esta vulnerabilidad, según la información publicada el pasado 21 de marzo por el desarrollador **Jacques Le Roux**, puede permitir a un atacante no autenticado ejecutar código de forma remota, comprometiendo de esta forma la confidencialidad, disponibilidad e integridad del sistema atacado.

A esta vulnerabilidad se le ha asignado el CVE-2021-26295 y afecta a la versión 17.12.05 y anteriores. Sin embargo, este error ya ha sido subsanado en la versión 17.12.06, por lo que se insta a los usuarios de dicha aplicación a actualizar lo antes posible.

ANÁLISIS TÉCNICO

La vulnerabilidad detectada en Apache OFBiz a la que se le ha asignado el CVE-2021-26295 se ha catalogado con una importancia crítica, ya que, puede permitir a un atacante no autenticado ejecutar código de forma remota. Este fallo se aprovecha de un error en el archivo *SafeObjectInputStream.java* que permite **modificar los datos serializados** para insertar código arbitrario. El tipo de vulnerabilidad del que se sirve este fallo para llegar a ejecutar código arbitrario es conocida como vulnerabilidad de deserialización de Java**.**

La serialización es un mecanismo para convertir el estado de un objeto en un flujo de bytes, por lo que se puede definir un objeto serializado en Java como una matriz de bytes con información que contiene el nombre del objeto al que se refiere y los datos del campo. El siguiente ejemplo muestra el objeto *ValueObject.ser* con un editor hexadecimal.

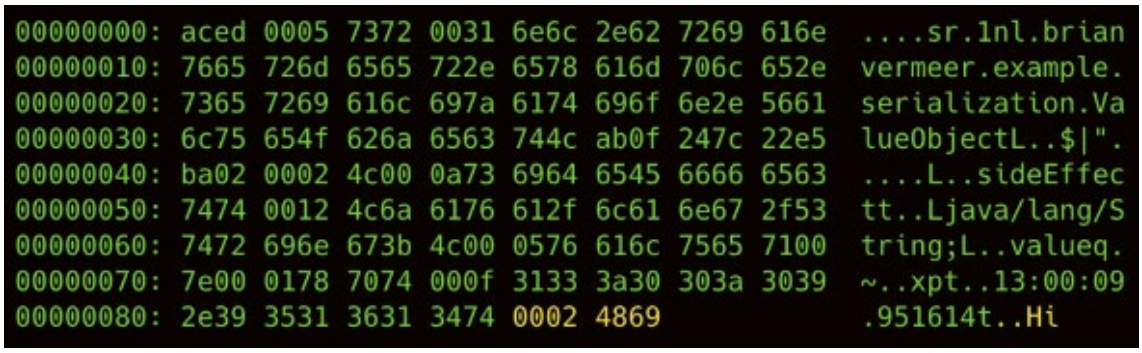

Imagen 1: Objeto serializado original

Sin embargo, la vulnerabilidad reportada permite modificar este objeto serializado e insertar en el mismo código arbitrario (se modifica Hi por Hallo, continuando con el ejemplo del objeto *ValueObject.ser*).

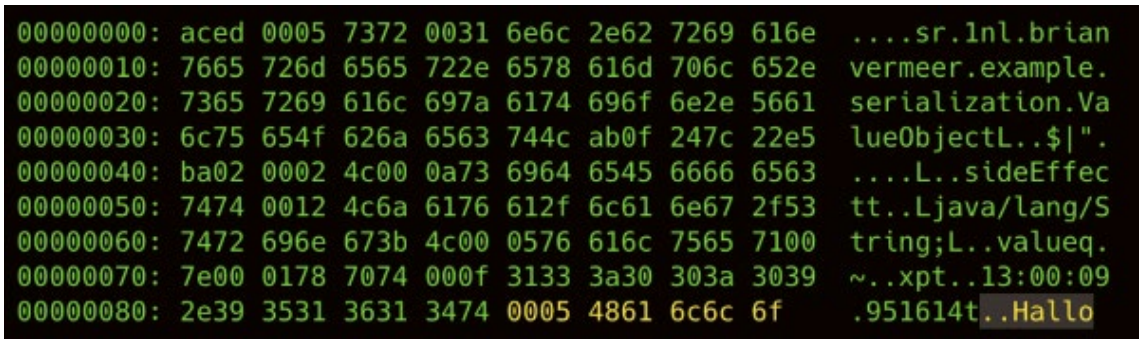

Imagen 2: Objeto serializado modificado

Esto implica que a la hora de realizar la deserialización del objeto, proceso inverso a la serialización en el que el flujo de bytes se utiliza para recrear el objeto Java real en memoria, se ejecuta el objeto modificado en lugar del original, dando lugar a la ejecución del código que se haya insertado en el objeto modificado por parte de los atacantes.

La base de datos del NIST ha registrado esta vulnerabilidad, pero por el momento no se le ha asignado puntuación de acuerdo con la escala CVSSv3. Por el momento no se han publicado exploits funcionales ni se ha detectado actividad que indique que la vulnerabilidad esté siendo explotada activamente. No obstante, el fallo expuesto anteriormente se ha catalogado como **crítico** por parte de los investigadores que lo han descubierto, por lo que conviene proceder a su actualización con urgencia.

MITIGACIÓN / SOLUCIÓN

La vulnerabilidad ya ha sido solucionada en la nueva versión **17.12.06** de Apache OFBiz publicada recientemente, por lo que se debe aplicar esta nueva versión en cuanto sea posible:

- https://www.apache.org/dyn/closer.lua/ofbiz/apache-ofbiz-17.12.06.zip

Por otro lado, destacar que el desarrollador Jacques Le Roux ha hecho público un parche para solventar esta vulnerabilidad, en caso de no ser posible actualizar a la versión indicada anteriormente:

- https://github.com/apache/ofbiz-framework/commit/af9ed4e/

Por último, y a modo informativo, se destacan varias formas de prevenir vulnerabilidades de deserialización de Java:

- Inspeccionar el objeto *ObjectInputStream* antes de deserializar.
- Utilizar la librería IO de Apache Commons. Esta librería proporciona un archivo llamado *ValidatedObjectInputStream* donde se puede indicar explícitamente los objetos que se desean deserializar, evitando que se deserialicen objetos inesperados.
- Utilizar la herramienta ysoserial. Colección de utilidades extremadamente útil para encontrar vulnerabilidades de deserialización de Java.

REFERENCIAS ADICIONALES

- The Apache OFBiz® Project - Release Notes 17.12.06
- The Apache OFBiz® Project - Downloads
- oss-sec: [CVE-2021-26295] RCE vulnerability in latest Apache OFBiz due to Java serialisation using RMI (seclists.org)
- NVD - CVE-2021-26295 (nist.gov)
- Critical RCE Vulnerability Found in Apache OFBiz ERP Software.
- Remote code execution in Apache OFBiz.

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?