ALERTA DE SEGURIDAD DE LA INFORMACIÓN
VULNERABILIDAD CRÍTICA DE INSECURE CONFIGURATION
EN SERVIDORES QUE USAN JBOSS 4.3.2

TLP: BLANCO

Descripción general de la vulnerabilidad

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior (CSIRT), ha detectado una vulnerabilidad crítica, identificada como *Insecure Configuration*, en sistemas desarrollados por terceros utilizando el servicio JBoss 4.3.2.

Debido al problema de configuración mencionado, es posible ejecutar código arbitrario en servidores que poseen instalada la aplicación JBoss sin necesidad de autentificación, debido a la exposición pública del controlador de Java Management Extensions (JMX) JMXInvokerServlet.

CVE identificados:

- CVE-2007-1036
- CVE-2010-0738
- CVE-2012-0874
- CVE-2013-4810
- CVE-2015-7501
- CVE-2017-10992

La vulnerabilidad es tipificada como A05:2021 Security Misconfiguration[1], y su debilidad es enumerada como CWE-15 External Control of System or Configuration Setting[2]. Esta última consiste en la exposición de uno o más sistemas de configuración, cuyo control puede ser tomado por un usuario no autorizado.

Esta vulnerabilidad se ha visto mencionada en CVE tales como CVE-2007-1036, CVE-2010-0738, CVE-2012-0874, CVE-2013-4810, CVE-2015-7501 y CVE-2017-10992.

En varios casos en que esta vulnerabilidad está presente, se ha encontrado hospedada en los servidores afectados una puerta trasera generada automáticamente por el script JexBoss, la cual permite la ejecución de código remoto con el mismo usuario asociado a la ejecución de la aplicación.

Además, se ha detectado que la interpretación de comandos derivada del payload de JexBoss se realiza con altos privilegios (usuario root), por lo que las capacidades de afectación e impacto superan todo control de seguridad previamente establecido.

[1] https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
[2] https://cwe.mitre.org/data/definitions/15.html

Como usuario root un atacante tendría la capacidad de realizar, entre otras cosas:

- Establecer un canal de comunicación remota con la máquina.
- Visualizar, modificar o destruir archivos de la máquina sin limitaciones.
- Cargar binarios maliciosos en el servidor web.
- Extraer y exfiltrar información sensible.
- Secuestrar el servidor web mediante Ransomware.
- Distribuir malware en la red interna y afectar a dispositivos adyacentes.

Mitigaciones

La amenaza a la que el sistema indicado se expone es crítica para las aplicaciones web. Por ese motivo se encuentra en los Top 10 de OWASP10[3], un proyecto que describe las 10 vulnerabilidades más frecuentes en los sitios web en el mundo.

Para resolver el problema descrito en este reporte, se recomienda fuertemente tomar las medidas de corto y largo plazo que se describen a continuación:

- En lo inmediato, es necesario determinar si el sitio web descrito presta servicios al público. De ser así: Actualizar sus tecnologías, desde el servidor web, lenguajes de programación, frameworks y API, entre otras implementaciones con las que cuente su aplicación y que puedan estar obsoletas o descontinuadas
    - Deshabilitar servicios
        - server/slim/deploy/jmx-invoker-adaptor-server.sar
        - server/slim/deploy/jmx-adaptor-plugin.jar
        - server/slim/deploy/jmx-console.war
    - Implemente prácticas de Threat Hunting y Threat Modeling para autenticaciones críticas, control de acceso, lógica de negocio y flujos clave.
    - Bloquear las entradas de rutas absolutas mediante uso de reglas en firewall de aplicación web (WAF).
        - /invoker/JMXInvokerServlet
        - /invoker/EBJInvokerServlet
- Si el sitio está descontinuado, es interno, está en desarrollo o se encuentra en cualquier otro estado en el que no es necesario que continúe en línea, se recomienda fuertemente sacarlo de línea. Si se requiere sólo internamente existen formas de publicarlo sólo para funcionarios del organismo correspondientes

A largo plazo, se recomienda lo siguiente:

- Si el desarrollo fue realizado con desarrolladores de la institución, se recomienda fuertemente capacitarlos para que adquieran la capacidad de corregir el código que pueda

[3] https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

ser vulnerable en los sistemas del ministerio, tanto aquellos expuestos en Internet (de forma prioritaria) como en aquellos internos.

- Si el desarrollo fue realizado a través de licitaciones externas, es necesario incluir en las licitaciones o contratos futuros cláusulas que obliguen a las empresas a incluir prácticas de desarrollo seguro, y a verificar el código entregado antes de ponerlo en producción.
- Actualizar las versiones de las aplicaciones que se utilicen es una práctica de seguridad fundamental. Es recomendable actualizar periódicamente las versiones de todo el software; de esa manera todo el sistema se va evaluando constantemente, verificando las compatibilidades del sistema y realizando las mitigaciones necesarias para que el sistema funcione con las versiones más recientes, entregando mayor seguridad al servidor y a los servicios.

Finalmente, es importante destacar la relevancia de las medidas preventivas para mitigar los riesgos, ya que la detección temprana y la implementación de medidas internas de seguridad sólidas para proteger la infraestructura tecnológica son clave al momento de defendernos contra amenazas de ciberseguridad cada vez más sofisticadas.

Ante cualquier inquietud sobre lo mencionado en este documento o las formas de detectar y mitigar la vulnerabilidad analizada, no dude en tomar contacto con el CSIRT a través de su correo electrónico incidentes@interior.gob.cl o su número telefónico corto 1510 (que es equivalente al +56 2 2486 3850).

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.11 16:30:53 -03'00'