Observatorio de Derechos Digitales

Software desactualizado en servicios gubernamentales

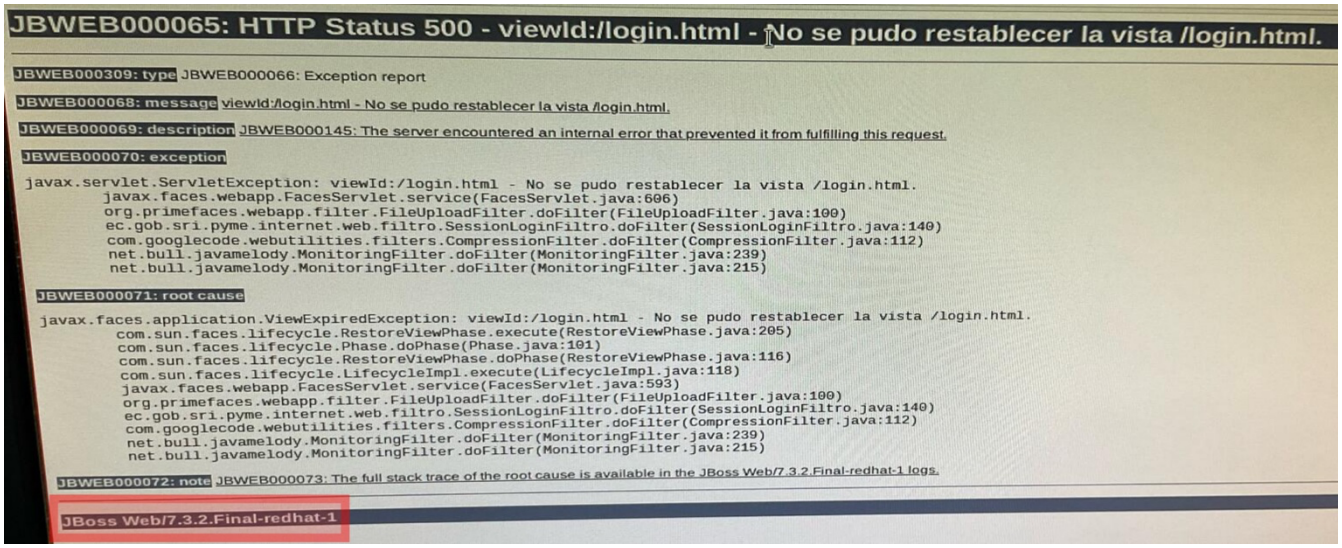
Alerta No. 4
Diciembre 2023

¿Qué es lo nuevo? Nueva evidencia muestra que los servicios gubernamentales, en este caso los del SRI [Servicio de Rentas Internas], dependen de software que no se ha actualizado durante más de diez años.

¿Por qué es importante? Este hecho es importante porque puede ser utilizado para atacar digitalmente servicios gubernamentales cruciales y robar o falsificar información importante, al mismo tiempo que muestra que el gobierno no tiene la competencia para gestionar sus propios sistemas. Asimismo, ésto abre preguntas sobre la integridad de las recientes elecciones y también la seguridad del resto del gobierno.

¿Qué debe hacerse? El sector público necesita invertir en asegurar su infraestructura, contratando personal técnico con experiencia en seguridad y agregar más presupuesto para educación en seguridad digital. En términos prácticos, mantener los sistemas actualizados a la última versión, realizar auditorías de seguridad periódicas y aplicar las mejores prácticas de seguridad, es crucial.

El lunes 30 de octubre de 2023, partes de los sistemas en línea del Servicio de Rentas Internas, SRI, experimentaron problemas. Esto resultó en que a los usuarios se les presenten informes de error al intentar autenticarse en el sistema de facturación del SRI (https://facturadorsri.sri.gob.ec). La respuesta específica se puede ver en la siguiente imagen:



Esta respuesta es generada por un sistema implementado en el lenguaje de programación Java. Al final de la página, es posible ver el software específico y la versión que es responsable de esta aplicación. Dice JBoss Web/7.3.2.Final-redhat-1. Esto especifica que el software es el JBoss Application Server y la versión en cuestión es 7.3.2.Final-redhat-1.

Esta versión de JBoss Web se puede encontrar en repositorios de un sistema de distribución llamado Maven. Pueden encontrar esta información en el repositorio canónico: https://mvnrepository.com/artifact/org.jboss.web/jbossweb y la información sobre la versión en cuestión se puede ver en https://mvnrepository.com/artifact/org.jboss.web/jbossweb/7.3.2.Final-redhat-1.

Hay dos detalles importantes. Primero, el artefacto (unidad instalable en el sistema Maven) específico se lanzó el 12 de junio de 2014. Y la última versión de este proyecto se lanzó el 21 de abril de 2018. En la sección de Red Hat GA que forma parte del repositorio, existe un artefacto que se lanzó el 1 de julio de 2020.

Después de investigar más, parece claro que los proyectos JBoss y JBoss Web han estado muertos durante algún tiempo y no ha recibido

actualizaciones durante muchos años. Sin embargo, 7.3.2 no es la última versión del software, lo que significa que la aplicación en cuestión no recibió actualizaciones incluso antes del final de la vida del proyecto.

¿Qué conclusiones podemos sacar de esta información? Primero, y más importante, una sección del software de este sistema no se ha actualizado en 9 años. No únicamente existen nuevas versiones, sino que el software en cuestión parece estar al final de su vida útil. Eso es lo único de lo que podemos estar seguros.

Sin embargo, también podemos suponer que el sistema operativo no se ha actualizado en este período de tiempo, ya que el software al que nos estamos refiriendo proviene de Red Hat, que es un proveedor de sistemas operativos. También podemos asumir que otras bibliotecas y componentes utilizados para este sistema no se han actualizado. Finalmente, la aplicación como tal, probablemente tampoco ha sido actualizada. La información en la imagen arriba expuesta implica el uso de tecnología bastante vieja.

Si esta aplicación y este servidor no se han actualizado durante mucho tiempo, ¿podemos concluir que es posible que otros sistemas del SRI estén sufriendo el mismo problema? ¿Podemos asumir también que otros sistemas gubernamentales estén en la misma situación? Ciertamente no podemos excluir la posibilidad. ¿Por qué es tan grave este problema? Porque el software siempre debe actualizarse para mantenerlo seguro. Los problemas de seguridad se descubren regularmente en bibliotecas y componentes del sistema operativo, y si no se realizan actualizaciones, esos defectos se pueden utilizar para atacar un sistema. Una búsqueda rápida mostrará que la versión en cuestión tiene vulnerabilidades conocidas. Y el sistema en cuestión almacena llaves privadas para el sistema de facturación electrónica. Un atacante podría utilizar las vulnerabilidades en cuestión, robar las llaves privadas y luego modificar la aplicación para almacenar todas las contraseñas ingresadas. Por lo que sabemos, es posible que esto ya haya sucedido.

Las actualizaciones periódicas de sistemas operativos, bibliotecas y aplicaciones son el primer paso para la seguridad. Todo lo demás es inútil sin actualizaciones.

Urge que el SRI haga una revisión de sus sistemas y trate de encontrar sistemas antiguos y los actualice. También deberían revisar la seguridad y verificar que no se hayan producido ataques. Además, la configuración de un sistema Java nunca debe mostrar una pantalla como la que se muestra en

la imagen. Revela demasiada información. La aplicación debe reconfigurarse para mostrar un mensaje de error genérico para el usuario y enviar la información específica al personal de TI.

Si eres usuario del sistema de facturación SRI, ¿hay algo que puedas hacer?
Lamentablemente no hay buenas opciones. El SRI sí cuenta con una aplicación pública para realizar facturación electrónica, pero no es software libre, lo que significa que estarías instalando software desconocido en tu máquina. El SRI debería publicar el código fuente de esta aplicación para que pueda ser revisada. Mientras tanto, existen empresas privadas que ofrecen sistemas de facturación. Estas son opciones pagadas y utilizarán el sistema SRI en un momento u otro, convirtiéndolas en alternativas sub-óptimas.

Si eres usuario del sistema de facturación SRI, ¿hay algo que puedas hacer? Lamentablemente no hay buenas opciones. El SRI sí cuenta con una aplicación pública para realizar facturación electrónica, pero no es software libre, lo que significa que estarías instalando software desconocido en tu máquina. El SRI debería publicar el código fuente de esta aplicación para que pueda ser revisada.

Lamentablemente, esta situación es difícil de evaluar. Se trata de un problema grave y es algo que el sector público debe investigar inmediatamente.

Además, si estás ofreciendo servicios privados a usuarios finales, también deberías revisar estos sistemas en busca de posible software desactualizado o problemático.

Actualmente, la tecnología forma la columna vertebral de las operaciones gubernamentales. Nuestros datos son recopilados, almacenados y utilizados de diversas formas. Sin embargo, aunque su uso puede ser muy provechoso el uso indebido o la falta de protección de estos datos plantea un riesgo significativo para los derechos y libertades de los individuos.

El caso reciente de los servicios gubernamentales del Servicio de Rentas Internas (SRI), que dependen de software no actualizado durante más de una década, sirve como un ejemplo alarmante de las implicaciones de la falta de actualización de software en el sector público. Esta desactualización

no solo contraviene los principios de la protección de datos, sino que también expone a los ciudadanos a una serie de riesgos significativos.

La falta de actualización de software puede llevar a la pérdida de control sobre la información personal. Los ciudadanos confían en que sus datos personales se manejarán de manera segura y confidencial por parte de las instituciones gubernamentales. Sin embargo, cuando los sistemas están desactualizados, esta confianza se ve socavada.

La confianza en las instituciones gubernamentales depende en gran medida de la percepción de que los datos personales están bajo un control seguro. La pérdida de control sobre información sensible mina la autonomía individual y plantea preguntas sobre la integridad de los servicios gubernamentales, esto puede tener consecuencias significativas para la gobernabilidad. Es, por tanto, un llamado urgente a la acción, un recordatorio de que la modernización tecnológica y la transparencia son esenciales para construir una administración pública eficiente y confiable.

La falta de actualización de software puede llevar a la pérdida de control sobre la información personal. Los ciudadanos confían en que sus datos personales se manejarán de manera segura y confidencial por parte de las instituciones gubernamentales. Sin embargo, cuando los sistemas están desactualizados, esta confianza se ve socavada.

Los fallos recurrentes en la prestación de servicios gubernamentales pueden erosionar **aún más** la confianza de los ciudadanos en la capacidad del gobierno para gestionar de manera efectiva y eficiente los asuntos críticos, e incluso los no tan críticos. Esta falta de confianza puede tener consecuencias a largo plazo en la percepción de la administración pública.

Los sistemas obsoletos también son propensos a errores y fallos técnicos. Esto puede tener un efecto paralizante en la prestación de servicios gubernamentales, lo que afecta la vida cotidiana de los ciudadanos. Los fallos en estos sistemas pueden, entre muchas cosas, afectar las operaciones comerciales y financieras de las empresas y personas naturales,

lo que a su vez afecta la economía en general.

Asimismo, además de los desafíos planteados, existen complejidades respecto a que los sistemas obsoletos suelen ser más complejos de mantener debido a la falta de estándares modernos y a la antigüedad de las prácticas de desarrollo. Esto puede dificultar la identificación y solución de errores, así como la implementación de nuevas funcionalidades.

La rápida evolución de la tecnología implica que los sistemas obsoletos pueden volverse incompatibles con hardware y software más recientes. Esta incompatibilidad puede dar lugar a conflictos y errores técnicos cuando se intenta integrar o interactuar con componentes más modernos del sistema.

Inclusive, los sistemas antiguos suelen presentar restricciones en lo que respecta a su capacidad de procesamiento, almacenamiento y velocidad de ejecución. Estas limitaciones pueden resultar en congestión del sistema y en la aparición de errores cuando se someten a cargas de trabajo más demandantes o a procesos más complicados.

Para abordar de manera efectiva los desafíos derivados de la obsolescencia de software en los servicios gubernamentales y garantizar la protección de datos, privacidad y derechos de los ciudadanos, el gobierno debe asumir un compromiso integral que abarque diversas áreas. Para ello es preciso preguntarse:

¿Cuáles son las acciones urgentes?

- Investigar la extensión de la desactualización de software en distintos sectores gubernamentales.
- Estudiar el impacto económico de los fallos técnicos y la interrupción de servicios causados por la desactualización de software en el sector público.
- Destinar recursos financieros significativos para la modernización de la infraestructura tecnológica gubernamental, asegurando la adopción de sistemas actualizados y seguros.

¿Qué hacer de aquí en adelante?

- Analizar casos internacionales para comparar la situación y las estrategias adoptadas por diferentes países frente a este problema.
- Adoptar un enfoque proactivo en la protección de datos en lugar de reaccionar a incidentes; es mandatorio implementar

sistemas de monitoreo continuo para detectar posibles amenazas.

- Realizar revisiones periódicas de seguridad y actualizaciones de software de acuerdo con un calendario establecido, y establecer mecanismos para recibir retroalimentación ciudadana sobre problemas de seguridad y privacidad.

Con el apoyo de:

Centro de Autonomía Digital

Orden Conflicto Violencia

Programa de Investigación