CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN Y SEGURO DE COOPERATIVAS DE PUERTO RICO

COSSEC

GOBIERNO DE PUERTO RICO

18 de noviembre de 2026

CARTA INFORMATIVA NÚM. 2026-28

A TODAS LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Mabel Jiménez Miranda, MBA
Presidenta Ejecutiva

ALERTA- FALLAS TECNOLÓGICAS

Reciban un cordial saludo.

COSSEC recuerda a las Cooperativas la importancia de mantener actualizados sus sistemas tecnológicos y fortalecer continuamente sus controles de seguridad informática. La atención oportuna a este tipo de vulnerabilidades resulta esencial para proteger la información institucional, los datos de los socios y la continuidad de los servicios financieros.

Asimismo, se recuerda que, de conformidad con las disposiciones del **Reglamento Núm. 9741 Sistemas de Información y Tecnología**, las Cooperativas deben mantener controles adecuados para la identificación, evaluación, mitigación y monitoreo de riesgos tecnológicos y de ciberseguridad.

En ese contexto, cada Cooperativa deberá evaluar esta vulnerabilidad como parte de sus procesos de administración de riesgos y activar, de ser necesario, los procedimientos establecidos en sus **planes de respuesta a incidentes,**

continuidad del negocio y recuperación ante desastres, a fin de garantizar la protección de los activos de información críticos y la continuidad de las operaciones esenciales.

Se exhorta a los Presidentes Ejecutivos y al oficial de seguridad de información a coordinar inmediatamente las acciones correspondientes con sus proveedores de servicios tecnológicos y equipos de ciberseguridad, según aplique. Asimismo, deberán documentar las medidas correctivas implementadas y mantener evidencia de las gestiones realizadas para atender esta vulnerabilidad, conforme a los requerimientos de gobernanza y cumplimiento aplicables.



Durante el día de ayer la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos *(Cybersecurity and Infrastructure Security Agency, CISA)* emitió una alerta sobre sobre una vulnerabilidad crítica de ciberseguridad identificada en Oracle Java titulada *Critical Java Vulnerability Requires Immediate Patching*.

La vulnerabilidad, identificada como **CVE-2026-114938**, denominada «Java4Shell», afecta el decodificador Base64 del entorno Java Virtual Machine (JVM), específicamente en la implementación x86-64 HotSpot, como parte del Java Development Kit (JDK).

Esta vulnerabilidad de corrupción de memoria podría provocar fallas en la máquina virtual y, mediante entradas Base64 especialmente diseñadas, permitir la ejecución remota de código sin autenticación, lo que representa un riesgo significativo para la seguridad de los sistemas y la información institucional.

ACCIONES REQUERIDAS

Ante la naturaleza crítica de esta vulnerabilidad, COSSEC exhorta conforme a las recomendaciones de *CISA* a todas las Cooperativas a tomar las siguientes medidas con carácter prioritario:

1. **Identificar los sistemas afectados:** Realizar un inventario y revisión de las instalaciones de Java, incluyendo JDK y Java Runtime Environments (JRE), así como aquellos integrados en aplicaciones de terceros, imágenes de contenedores y equipos institucionales.
2. **Aplicar las actualizaciones de seguridad:** Gestionar e instalar los parchos de seguridad correspondientes emitidos por Oracle y los respectivos suplidores de tecnología, tan pronto estén disponibles. Se deberá dar prioridad a los sistemas expuestos a internet.
3. **Implementar medidas de mitigación temporeras:** Cuando no sea posible aplicar inmediatamente las actualizaciones, establecer controles compensatorios, incluyendo restricciones a las entradas Base64, validación de datos en los puntos de acceso de las aplicaciones, límites al tamaño de las entradas y restricciones al acceso no autenticado.
4. **Evaluar las recomendaciones del fabricante:** Revisar el aviso de seguridad de Oracle para identificar los productos y versiones afectados, así como las instrucciones correspondientes para atender la vulnerabilidad.
5. **Monitorear actividades sospechosas:** Reforzar los mecanismos de monitoreo para identificar posibles indicadores de compromiso, incluyendo procesos Java no autorizados, fallas inesperadas de la JVM y comportamientos anómalos en las aplicaciones.

Hacemos un llamado a todas las Cooperativas a mantener mecanismos efectivos de monitoreo y gestión de riesgo de terceros ante eventos de ciberseguridad que puedan surgir en el ecosistema tecnológico y financiero.

Agradecemos su cooperación y compromiso con la seguridad del sistema cooperativo. Si tienen alguna pregunta pueden comunicarse al Área de Apoyo Técnico y Supervisión con el Sr. Luis Ortiz Sánchez al 787-622-0957, extensión 1412, o mediante correo electrónico a laortiz@cossec.prgov.

RECURSOS DE REFERENCIA

Para información adicional y orientación técnica, se recomienda consultar los siguientes recursos:



- CISA: *Critical Java Vulnerability Requires Immediate Patching*.
- Oracle: *Critical Security Patch Update – November 2026*.

Agradecemos su atención y cooperación ante este asunto de alta prioridad para la seguridad y estabilidad operacional del sector cooperativo.