Nro. Alerta:	EC-2022-61	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	27-abril-2022	**Vulnerabilidad Criptográfica de Java**	Versión 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades
Tipo de incidente: Sistema o Software Abierto
Nivel de riesgo: Alto

II. ALERTA

En ciertos productos de Java se presenta una vulnerabilidad en la omisión de firma digital que podría permitir a un atacante falsificar firmas y eludir las medidas de autenticación implementadas; permitiendo la modificación de comunicaciones.

Figura 1. Ilustración relacionada a productos afectados de Java
Fuente: Java

III. INTRODUCCIÓN

Oracle, a través del aviso de actualización de parches críticos de abril de 2022; dio a conocer un total de 520 nuevos parches; sin embargo, entre estas múltiples vulnerabilidades, una vulnerabilidad identificada bajo CVE-2022-21449 llama plenamente la atención; debido a una omisión de firma digital en ciertos productos de Java.

Esta vulnerabilidad, calificada de alta gravedad (puntaje CVSS: 7.5) afecta a las siguientes versiones:

- Oracle Java SE: 17.0.2, 18.
- Oracle GraalVM Enterprise Edition: 21.3.1, 22.0.0.2.

Es decir, la afectación se origina en una implementación incorrecta del algoritmo de verificación de firma ECDSA (Algoritmo de Firma Digital de Curva Elíptica) y esencialmente permite que un atacante intercepte potencialmente comunicaciones y mensajes que de otro modo deberían haber sido encriptados, como la comunicación SSL.

En este sentido, CVE-2022-21449 hace alusión a un error criptográfico (Psychic Signatures en Java) que permitiría presentar una firma totalmente en blanco, que aún sería percibida como válida; así mismo, permitiría falsificar firmas y eludir las medidas de autenticación implementadas.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-61	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	27-abril-2022	**Vulnerabilidad Criptográfica de Java**	Versión 1.1

IV. VECTOR DE ATAQUE:

En al siguiente tabla, se describe el vector de ataque asociado a estas vulnerabilidades.

Ítem	CVE asociado	Descripción Vector de Ataque	String Vector
1	CVE-2022-21449	Un atacante no autenticado con acceso a la red a través de múltiples protocolos puede comprometer a Oracle Java SE, Oracle GraalVM Enterprise Edition; permitiendo a un atacante falsificar firmas y eludir las medidas de autenticación implementadas.	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Tabla 1. Vector de ataque de vulnerabilidades
Fuente: JAVA

V. IMPACTO:

A continuación, se mencionan los impactos asociados a la vulnerabilidad en productos VMware.

Ítem	CVE asociado	Afectación	Impacto
6	CVE-2022-21449	Provoca la anulación de la integridad de cualquier contenido que esté garantizado por firmas electrónicas	Confidencialidad: Ninguna Integridad: Alta Disponibilidad: Ninguna

Tabla 2. Impacto de vulnerabilidades
Fuente: JAVA

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar las respectivas actualizaciones entregadas por el proveedor.
- Mantener actualizado los productos de seguridad.
- Emplear conexiones seguras.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-61	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	27-abril-2022	**Vulnerabilidad Criptográfica de Java**	Versión 1.1

VII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

Greig, J. (23 de 04 de 2022). *The Record*. Obtenido de The Record: https://therecord.media/experts-warn-of-need-to-patch-critical-cryptographic-java-bug/

Madden, N. (19 de 04 de 2022). *Neil Madden*. Obtenido de Neil Madden: https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/

Oracle. (04 de 2022). *Oracle Critical Patch Update Advisory*. Obtenido de Oracle Critical Patch Update Advisory: https://www.oracle.com/security-alerts/cpuapr2022.html

RedHat. (19 de 04 de 2022). *Red Hat Customer Portal*. Obtenido de Red Hat Customer Portal: https://access.redhat.com/security/cve/cve-2022-21449

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec