Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-dic-2021	**Actualización de Información: Vulnerabilidad en Apache Log4j**	V 1.3

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Desde la publicación de la vulnerabilidad en Apache Log4j, se ha dado a conocer varias vulnerabilidades asociadas al CVE-2021-44228; las cuales han sido corregidas en la última versión lanzada por Apache.

Figura No. 1.- lustraciones distintivas de Apache.
Fuente: Apache

III. INTRODUCCIÓN

El Centro de Respuestas de la Agencia de Regulación y Control de la Telecomunicaciones, EcuCERT, cumpliendo su misión de servir a su comunidad objetivo, en la prevención de incidentes de seguridad de la información; ha compartido información relacionada sobre la vulnerabilidad en Apache Log4j, la cual puede ser encontrada en los siguientes links:

- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4j-2.pdf
- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4j-actualizacion-3.pdf
- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4s-update3.pdf

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-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-dic-2021	**Actualización de Información: Vulnerabilidad en Apache Log4j**	V 1.3

IV. VECTOR DE ATAQUE: Red

Esta vulnerabilidad del tipo RCE (Ejecución Remota de Código) se produce al momento en el que la función “log4j2.formatMsgNoLookups”, la cual se encuentra en la librería JNDI de Java, no verifica adecuadamente el valor cargado. Es decir, el atacante puede enviar una petición especialmente diseñada para lograr que el servidor afectado descargue y almacene una clase Java maliciosa, la cual le permite ejecutar código arbitrario sobre el servidor afectado. (Informáticos, 2021)

V. IMPACTO:

Múltiples fabricantes se encuentran actualizando información relacionada a esta vulnerabilidad, la misma que puede ser encontrada en:

- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4j-2.pdf
- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4j-actualizacion-3.pdf
- https://www.ecucert.gob.ec/wp-content/uploads/2021/12/alerta-log4s-update3.pdf

Así mismo, en el siguiente enlace; se encuentra información detallada de la vulnerabilidad, el fabricante y el actual estado.

- https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md

VI. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de la ARCOTEL, EcuCERT, recomienda tomar en consideración lo siguiente:

- Para todas las versiones se recomienda actualizar Log4J.
- En el caso que no se pueda actualizar el software de manera oportuna se sugiere desinstalar o deshabilitar Log4j hasta que se puedan aplicar las actualizaciones, así también como aislar el sistema.

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-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	
TLP:	TLP:BLANCO		
Fecha:	28-dic-2021	**Actualización de Información: Vulnerabilidad en Apache Log4j**	V 1.3

VII. REFERENCIAS:

- Apache. (17 de 12 de 2021). Recuperado el 28 de diciembre de 2021. Obtenido de Apache: https://logging.apache.org/log4j/2.x/security.html
- Github. (20 de 12 de 2021). Github. Recuperado el 28 de diciembre de 2021. Obtenido de Github: https://github.com/cisagov/log4j-affected-db
- Informáticos, C. N. (22 de 12 de 2021). Centro Nacional de Respuesta a Incidentes Informáticos. Recuperado el 28 de diciembre de 2021. Obtenido de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/vulnerabilidad-log4j

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