Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Desde el 9 de diciembre de 2021; fecha en la que fue dada a conocer la vulnerabilidad CVE-2021-44228, diferentes sitios WEB han dado a conocer información y soluciones a esta problemática; sin embargo a la presente fecha, se ha detectado variantes como la CVE-2021-45105 –nueva tipología de denegación de servicio DoS-; razón por la cual se recomienda instalar nuevos parches, en este caso el 2.17.

Figura 1.- Ilustraciones distintivas de Log4j.
Fuente: Apache

III. INTRODUCCIÓN

El Ecucert a través de su página Web ha actualizado constantemente información sobre la vulnerabilidad en Apache Log4j; en este sentido, en el presente reporte se mencionan características difundidas en los últimos días en relación a esta vulnerabilidad.

IV. VECTOR DE ATAQUE: RED

Esta vulnerabilidad afecta a las versiones de Log4j anteriores a 2.16.0; estando sujetas a

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 DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

ejecución remota de código a través del analizador ldap JNDI.

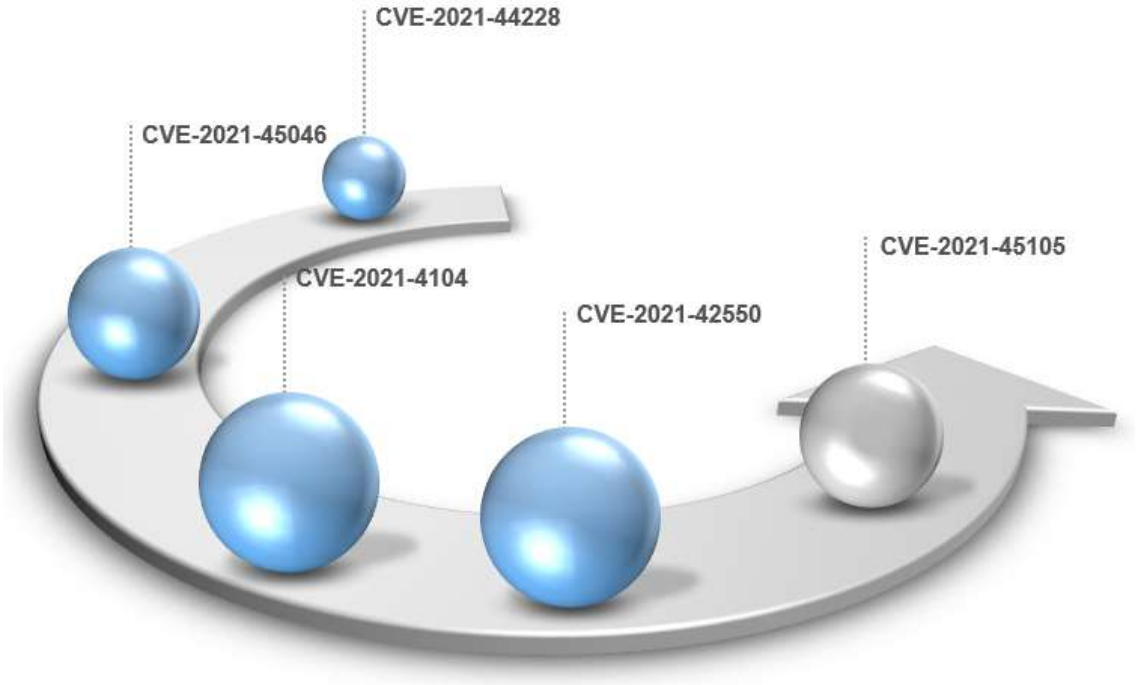

Figura 2.- CVE asociado a vulnerabilidad Log4j
Fuente: NATIONAL VULNERABILITY DATABASE

A continuación se listan las fallas descubiertas:

Tabla 1. CVE asociadas

CVE	BASE SCORE	VECTOR	DESCRIPCIÓN
CVE-2021-44228	10 Crítico	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	Otorga capacidades de ejecución remota de código (RCE) a atacantes no autenticados, lo que permite la toma de control completa del sistema. Desde la versión 2.16.0, esta funcionalidad se ha eliminado por completo. Tenga en cuenta que esta vulnerabilidad es específica de log4j-core y no afecta a log4net, log4cxx ni a otros proyectos de Apache Logging Services.

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 DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

CVE	BASE SCORE	VECTOR	DESCRIPCIÓN
CVE-2021-45046	9.0 Crítico	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	La falla surgió como resultado de una solución incompleta para CVE-2021-44228. Este es un defecto de Denegación de Servicio (DoS). Log4j 2.16.0 (Java 8) y 2.12.2 (Java 7) solucionan este problema al eliminar la compatibilidad con los patrones de búsqueda de mensajes y deshabilitar la funcionalidad JNDI de forma predeterminada.
CVE-2021-4104	8.1 Alta	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	JMSAppender en Log4j 1.2 es vulnerable a la deserialización de datos que no son de confianza cuando el atacante tiene acceso de escritura a la configuración de Log4j. El atacante puede proporcionar configuraciones TopicBindingName y TopicConnectionFactoryBindingName, lo que hace que JMSAppender realice solicitudes JNDI que dan como resultado la ejecución remota de código de manera similar a CVE-2021-44228. Este problema solo afecta a Log4j 1.2 cuando se configura específicamente para usar JMSAppender, que no es el predeterminado. Apache Log4j 1.2 llegó al final de su vida útil en agosto de 2015. Los usuarios deben actualizar a Log4j 2, ya que resuelve muchos otros problemas de las versiones anteriores.
CVE-2021-42550	6.6 Medium	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H	Vulnerabilidad en el framework Logback, un sucesor de la biblioteca Log4j 1.x. CVE-2021-4104 también afectaba a Log4j 1.x, y se evaluó la posibilidad de un impacto potencial en Logback. Se han lanzado versiones más recientes de Logback v1.3.0-alpha11 y v1.2.9 que abordan esta vulnerabilidad menos grave.

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 DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

CVE	BASE SCORE	VECTOR	DESCRIPCIÓN
CVE-2021-45105	7.5 Alto	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H	Se descubrió que Log4j 2.16.0 era vulnerable a una falla DoS. Desde entonces, Apache ha lanzado una versión log4j 2.17.0 que corrige el CVE.

Fuente: NATIONAL VULNERABILITY DATABASE

V. IMPACTO:

Los impactos de esta vulnerabilidad pueden encontrarse en:

- 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-log4j-2.pdf

Así mismo, en el Blog de Seguridad de Google; se menciona que: *"… Más de 35.000 paquetes de Java, que representan más del 8% del repositorio de Maven Central (el repositorio de paquetes de Java más importante), se han visto afectados por las vulnerabilidades log4j reveladas recientemente… "*

Cabe señalar que esta vulnerabilidad está siendo explotada con más aplicativos; por ejemplo ciberseguridad Cryptolaemus; advirtió que la vulnerabilidad Log4j ahora se explota para infectar dispositivos Windows con el troyano Dridex y dispositivos Linux con Meterpreter permitiendo una propagación en la red, robar datos o implementar ransomware.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Determine si los productos de su organización con Log4j son vulnerables:
  Según la "Guía de vulnerabilidad de Apache Log4j" elaborada por CISA (Cybersecurity & Infraestructure Security Agency) sugiere seguir el siguiente cuadro de análisis.

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 DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

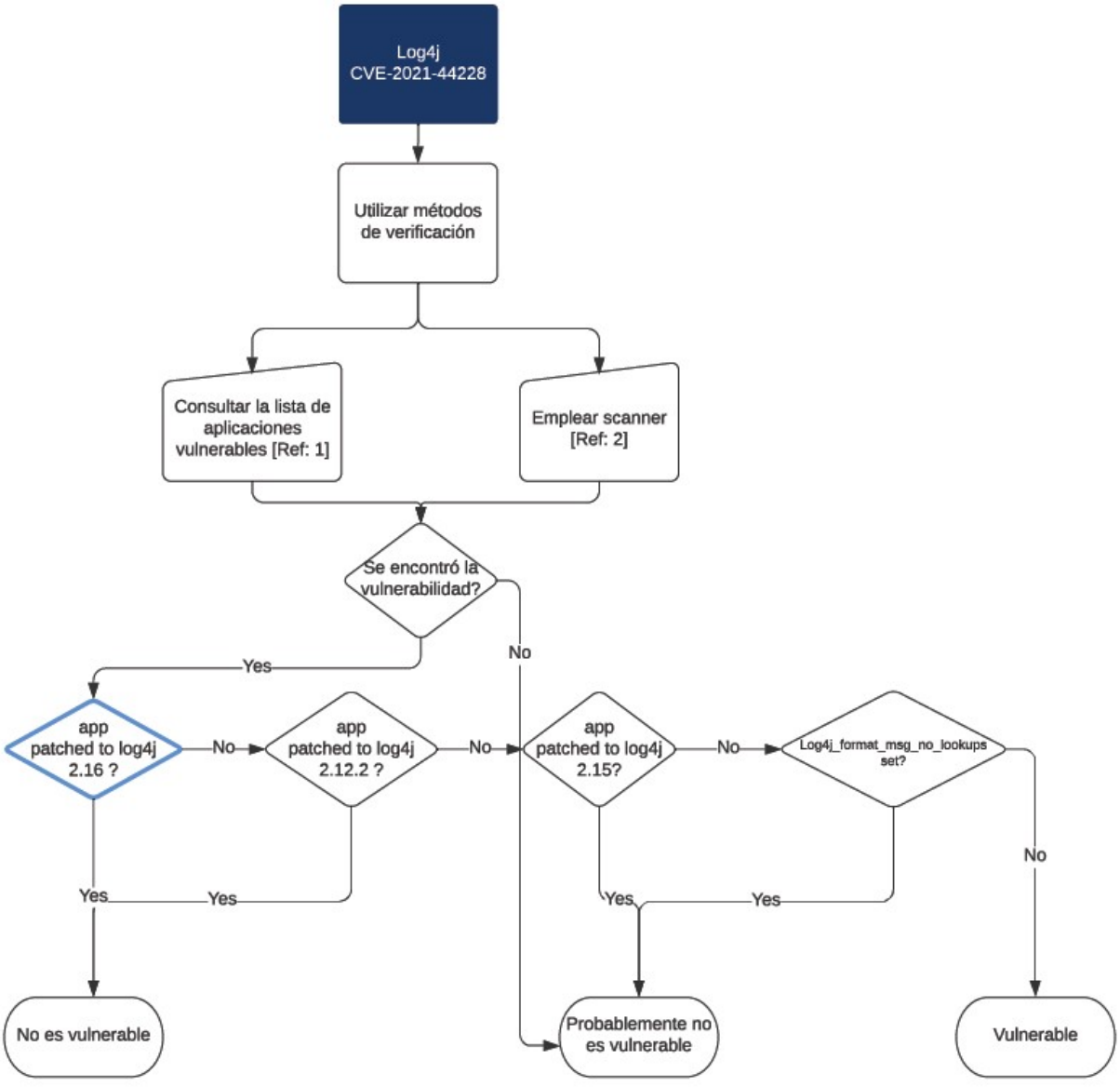

Figura 3.- Diagrama de flujo para determinar vulnerabilidad log4j.
Fuente: CISA

Siendo:

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 DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

Referencia 1: https://github.com/cisagov/log4j-affected-db
Referencia 2: https://github.com/CERTCC/CVE-2021-44228_scanner

- Parchear inmediatamente cualquier instancia de Log4j a 2.17.0.
- 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.

VII. REFERENCIAS:

Apache. (17 de 12 de 2021). Obtenido de Apache: https://logging.apache.org/log4j/2.x/security.html

Apache Log4j 2. (17 de 12 de 2021). Obtenido de Apache Log4j 2: https://logging.apache.org/log4j/2.x/

bleepingcomputer. (10 de 12 de 2021). Obtenido de bleepingcomputer: https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/

Blog de Seguridad de Google. (17 de 12 de 2021). Obtenido de Blog de Seguridad de Google: https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html

blog elhacker net. (20 de 12 de 2021). Obtenido de blog elhacker net: https://blog.elhacker.net/2021/12/resumen-de-todas-las-vulnerabilidades-log4j-log4shell.html

Center for Internet Security. (20 de 12 de 2021). Obtenido de Center for Internet Security: https://www.cisecurity.org/log4j-zero-day-vulnerability-response/

CISA. (18 de 12 de 2021). Obtenido de CISA: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

CN CERT. (20 de 12 de 2021). Obtenido de CN CERT: https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/11435-ccn-cert-al-09-21-vulnerabilidad-en-apache-log4j-2.html

NATIONAL VULNERABILITY DATABASE. (10 de 12 de 2021). Obtenido de NATIONAL VULNERABILITY DATABASE: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

NATIONAL VULNERABILITY DATABASE. (14 de 12 de 2021). Obtenido de NATIONAL

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.2

VULNERABILITY DATABASE: https://nvd.nist.gov/vuln/detail/CVE-2021-45046

NATIONAL VULNERABILITY DATABASE. (14 de 12 de 2021). Obtenido de NATIONAL VULNERABILITY DATABASE: https://nvd.nist.gov/vuln/detail/CVE-2021-4104#vulnCurrentDescriptionTitle

NATIONAL VULNERABILITY DATABASE. (16 de 12 de 2021). Obtenido de NATIONAL VULNERABILITY DATABASE: https://nvd.nist.gov/vuln/detail/CVE-2021-42550

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