Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	18-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

En diferentes sitios Web y en los canales de difusión del Ecuacert; se han dado a conocer características técnicas asociadas a Log4j, la misma que se ha denominado Log4Shell o LogJam, y fue descubierta el pasado 9 de diciembre de 2021.

En este sentido, los diferentes equipos de seguridad de diferentes empresas han empezado a "parchar", la vulnerabilidad CVE-2021-44228 para evitar diferentes tipos de ataques

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

III. INTRODUCCIÓN

A través de la página del Ecucert, se dio a conocer las características de la "Vulnerabilidad grave en #Apache Log4j 2."; a continuación, se mencionan características difundidas en los últimos días en relación a esta vulnerabilidad.

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:	18-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.1

IV. VECTOR DE ATAQUE: RED

Esta vulnerabilidad permite la ejecución remota de código no autenticado y se activa cuando el componente vulnerable **Log4j 2** analiza y procesa una cadena especialmente diseñada proporcionada por el atacante a través de una variedad de diferentes vectores de entrada; es decir, se puede explotar a través de una red sin necesidad de credenciales de usuario.

En la figura 2, se observa un escenario normal de respuesta de Log4j; así mismo, se observa como un atacante realiza una solicitud HTTP, que genera un registro utilizando Log4j que aprovecha JNDI para realizar una solicitud al sitio contralado por el atacante.

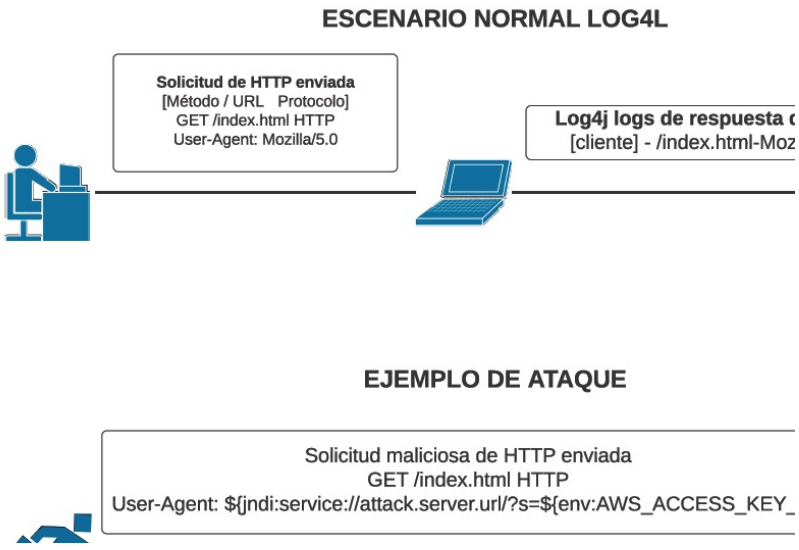

Figura 2.- Escenario Normal y ejemplo de ataque de Log4Shell
Fuente: Sophos News

Así mismo, se ha observado que varios actores de amenazas aprovechan la vulnerabilidad CVE-2021-44228 en ataques activos; a continuación se listan las fallas descubiertas:

Tabla 1. CVE asociadas

CVE	DESCRIPCIÓN
CVE-2021-45046	Una fuga de información y una vulnerabilidad de ejecución remota de código que afecta a las versiones de Log4j de 2.0-beta9 a 2.15.0, excluyendo 2.12.2 (corregida en la versión 2.16.0).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec
Gobierno del Encuentro | Juntos lo logramos

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	18-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.1

CVE-2021-45105	Vulnerabilidad de denegación de servicio que afecta a las versiones de Log4j de 2.0-beta9 a 2.16.0 (corregida en la versión 2.17.0).
CVE-2021-45104	Falla de deserialización no confiable que afecta a la versión 1.2 de Log4j (aún no hay solución disponible. Se recomienda actualizar a la versión 2.17.0)

Fuente: CSIRT CHILE

V. IMPACTO:

Diferentes fabricantes que emplean en sus productos la librería Log4j2 están actualizando información de sus productos afectados y algunos de ellos mencionan soluciones. En la siguiente Tabla, se indican los fabricantes y los productos afectados.

Tabla 2. Fabricantes y productos afectados

FABRICANTE	PRODUCTOS AFECTADOS
Apache Solr	https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228
Apache Struts	https://struts.apache.org/announce-2021#a20211212-2
Atlassian	https://confluence.atlassian.com/kb/faq-for-cve-2021-44228-1103069406.html
BMC	https://community.bmc.com/s/news/aA33n000000TSUdCAO/bmc-security-advisory-for-cve202144228-log4shell-vulnerability
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
Citrix	https://support.citrix.com/article/CTX335705
Debian	https://security-tracker.debian.org/tracker/CVE-2021-44228
Docker	https://www.docker.com/blog/apache-log4j-2-cve-2021-44228/
F-Secure	https://status.f-secure.com/incidents/sk8vmr0h34pd
Fortinet;	https://www.fortiguard.com/psirt/FG-IR-21-245

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:	18-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j**	V 1.1

RedHat	https://access.redhat.com/security/cve/cve-2021-44228
Solarwinds	https://www.solarwinds.com/trust-center/security-advisories/cve-2021-44228
VMware	https://www.vmware.com/security/advisories/VMSA-2021-0028.html

Fuente: Incibe-Cert

Así mismo, el portal GitHub, publica un listado ampliado de los diferentes fabricantes y las implicaciones que presenta esta vulnerabilidad. En el enlace: https://github.com/NCSC-NL/log4shell/blob/main/software/README.md se encuentra la información a mayor detalle.

VI. RECOMENDACIONES:

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

- Revisar si está usando Log4j

Tabla 2. Fabricantes y productos afectados

Power Shell	https://github.com/crypt0jan/log4j-powershell-checker gci 'C:\' -rec -force -include *.jar -ea 0 | foreach {select-string "JndiLookup.class" $_} | select -exp Path
Linux	find / 2>/dev/null -regex ".*.jar" -type f | xargs -I{} grep JndiLookup.class "{}" Revisar ficheros de configuración buscando log4j2.formatMsgNoLookups y la variable de entorno LOG4J_FORMAT_MSG_NO_LOOKUPS. Deben estar a True.
Revisar aplicaciones de Java	https://github.com/logpresso/CVE-2021-44228-Scanner
Escaneo de vulnerabilidad en Go	https://github.com/hillu/local-log4j-vuln-scanner

Fuente: CN-Cert

- Como medidas de mitigación, en versiones anteriores (>=2.10) este comportamiento puede mitigarse estableciendo la propiedad del sistema: **log4j2.formatMsgNoLookups = true** o eliminando la clase ***JndiLookup*** del *classpath*.

- También puede mitigarse eliminando la clase JndiLookup del classpath,: **zip -q -d**

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec
Gobierno del Encuentro | Juntos lo logramos

log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

- Java 8u121 recomienda establecer por defecto:
  com.sun.jndi.rmi.object.trustURLCodebase = false
  com.sun.jndi.cosnaming.object.trustURLCodebase = false

- Revisar si existe un aumento de conexiones DNS, ya que un aumento fuera de lo habitual en las conexiones salientes a DNS puede ser indicativo de explotación exitosa.

- Revisar las medidas de mitigación descritas por los diferentes fabricantes en la Tabla 2 del presente documento.

VII. REFERENCIAS:

CN CERT. (14 de 12 de 2021). Obtenido de https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/11435-ccn-cert-al-09-21-vulnerabilidad-en-apache-log4j-2.html

CSIRT CHILE. (18 de 12 de 2021). Obtenido de https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00535-01/

GitHub. (s.f.). Obtenido de https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

INCIBE-CERT. (13 de 12 de 2021). Obtenido de https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/log4shell-vulnerabilidad-0day-ejecucion-remota-codigo-apache-log4j

SEGU.INFO. (16 de 12 de 2021). Obtenido de https://blog.segu-info.com.ar/2021/12/tercera-vulnerabilidad-en-log4j.html

Seguridad de Microsoft. (15 de 12 de 2021). Obtenido de https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Sohpos News. (12 de 12 de 2021). Obtenido de https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/