Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	13-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j 2.**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Los diferentes equipos de seguridad de diferentes empresas han empezado a “parchar”, la vulnerabilidad CVE-2021-44228 para evitar diferentes tipos de ataques.

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

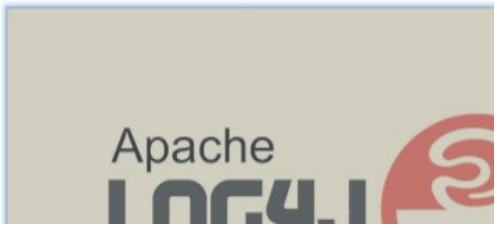

Figura 1.- lustraciones distintivas de Log4Shell
Fuente: Apache

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 describen mayores 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:	13-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j 2.**	V 1.1

IV. VECTOR DE ATAQUE: RED

Esta vulnerabilidad se puede explotar de forma remota sin autenticación, es decir, se puede explotar a través de una red sin necesidad de credenciales de usuario.

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.

Figura 1. 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
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:	13-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j 2.**	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:

- Como medidas de mitigación, en versiones anteriores (>=2.10) este comportamiento puede mitigarse estableciendo la propiedad del sistema: **log4j2.formatMsgNoLookups = true**
- También puede mitigarse eliminando la clase JndiLookup del classpath,: **zip -q -d 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 las medidas de mitigación descritas por los diferentes fabricantes en la Tabla 1 del presente documento.

VII. REFERENCIAS:

- 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

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:	13-dic-2021	**Actualización de Información Vulnerabilidad en Apache Log4j 2.**	V 1.1

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