
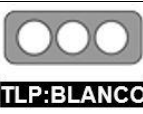


| | | | |
|-----------------|--|--|---|
| Código: | 09VSA-20211211-01 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD |  |
| Fecha: | 11-dic-2021 | | |
| TLP |  TLP:BLANCO | | |
| Versión: | 1.0 | Vulnerabilidad grave en #Apache Log4j 2. | |

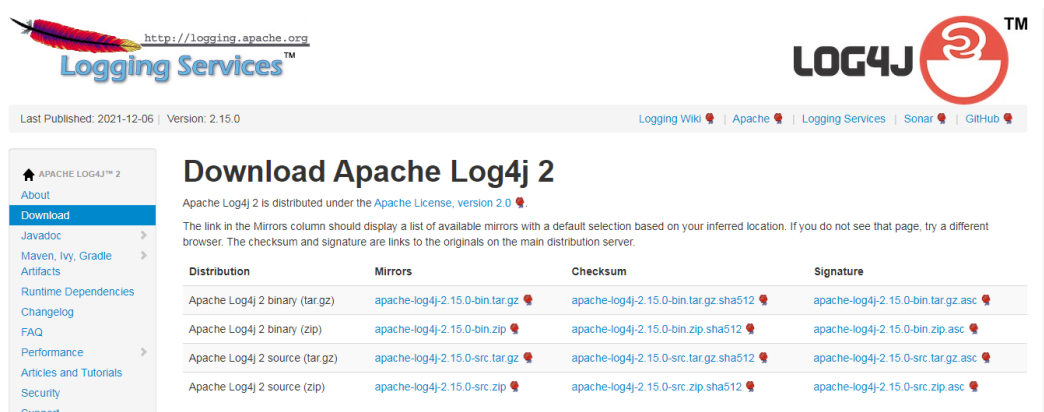
I. DATOS GENERALES:

| | |
|----------------------------|-------------------------------|
| Clase de Incidente: | Vulnerabilidad |
| Tipo de incidente: | Sistemas y/o software Abierto |
| Nivel de riesgo: | Alto |

II. INTRODUCCIÓN

Varios sitios Web informan de una vulnerabilidad crítica CVE-2021-44228 en Log4Shell o LogJam; siendo esta una vulnerabilidad RCE [Ejecución Remota de Código] que afecta diferentes configuraciones predeterminadas de Apache, incluidos Apache Struts2, Apache Solr, Apache Druid y Apache Flink, utilizados por varios productos de software empresarial.

Es importante considerar que, Log4j es una librería adicional desarrollada en Java por Apache Software Foundation y es usada en diferentes aplicaciones empresariales de Apple, Amazon, Cloudflare, Twitter, Steam y servicios en la nube.



Logging Services™ <http://logging.apache.org>

LOG4J™

Last Published: 2021-12-06 | Version: 2.15.0

Logging Wiki | Apache | Logging Services | Sonar | GitHub



Download Apache Log4j 2

Apache Log4j 2 is distributed under the Apache License, version 2.0.

The link in the Mirrors column should display a list of available mirrors with a default selection based on your inferred location. If you do not see that page, try a different browser. The checksum and signature are links to the originals on the main distribution server.

| Distribution | Mirrors | Checksum | Signature |
|--------------------------------|--|---|--|
| Apache Log4j 2 binary (tar.gz) | apache-log4j-2.15.0-bin.tar.gz | apache-log4j-2.15.0-bin.tar.gz.sha512 | apache-log4j-2.15.0-bin.tar.gz.asc |
| Apache Log4j 2 binary (zip) | apache-log4j-2.15.0-bin.zip | apache-log4j-2.15.0-bin.zip.sha512 | apache-log4j-2.15.0-bin.zip.asc |
| Apache Log4j 2 source (tar.gz) | apache-log4j-2.15.0-src.tar.gz | apache-log4j-2.15.0-src.tar.gz.sha512 | apache-log4j-2.15.0-src.tar.gz.asc |
| Apache Log4j 2 source (zip) | apache-log4j-2.15.0-src.zip | apache-log4j-2.15.0-src.zip.sha512 | apache-log4j-2.15.0-src.zip.asc |

Figura 1. Sitio Web de Descargas de Apache
Fuente: Apache

| | | | |
|----------|--|--|---|
| Código: | 09VSA-20211211-01 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD |  |
| Fecha: | 11-dic-2021 | | |
| TLP |  TLP:BLANCO | | |
| Versión: | 1.0 | Vulnerabilidad grave en #Apache Log4j 2. | |

III. 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.

IV. IMPACTO:

- CVSS 3.1 Base Score 10.0 (impactos de confidencialidad, integridad y disponibilidad)
- Como se mencionó anteriormente, el producto afectado es Apache Log4j 2 versiones 2.0 a 2.14.1.

V. RECOMENDACIONES:

El Centro de Respuesta a Incidentes Informáticos EcuCERT, recomienda:

- Actualizar versiones de versiones de log4j a log4j-2.15.0
- Aplicar actualizaciones oficiales del sitio <https://logging.apache.org/log4j/2.x/download.html>
- Revisar Logs de aplicaciones relacionadas a Apache Log4j 2.
- Revisar periódicamente cualquier actividad maliciosa asociada con CVE-2021-44228.

VI. REFERENCIAS:

BleepingComputer. (10 de 12 de 2021). Obtenido de <https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-log4j-java-library-is-an-enterprise-nightmare/>

Diario Informe. (s.f.). Obtenido de <https://diarioinforme.com/minecraft-lanza-un-parche-para-la-vulnerabilidad-critica-de-log4j/>

ORACLE. (s.f.). Obtenido de <https://www.oracle.com/security-alerts/alert-cve-Loggin-Services.> (06 de 12 de 2021). Obtenido de <https://logging.apache.org/log4j/2.x/download.html2021-44228.html>