**OUTBREAK ALERTS**

# Log4j2 Vulnerability

## RCE and DoS in Apache Java logging library

https://logging.apache.org/log4j/2.x/security.html
CVEs: CVE-2021-44228 CVE-2021-45046 CVE-2021-45105 CVE-2021-44832

A 0-day exploit was discovered on a popular Java library Log4j2 that can result to a Remote Code Execution (RCE). This is a widely deployed library, and while systems protected by Fortinet Security Fabric are secured by the protections below, all systems need to upgrade ASAP as this is 10.0 severity. Due to the high visibility and attention, subsequent vulnerabilities have since emerged.

**Background**

The Log4j2 is a Java-based logging utility that is part of the Apache Software. Detailed background is available in the Fortinet Blog:
https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know
If you are looking for information pertaining to Fortinet products impacted by this vulnerability, refer to:
https://www.fortiguard.com/psirt/FG-IR-21-245?utm_source=blog&utm_campaign=blog
And, for more technical information pertaining to each vulnerability , please refer to the FortiGuard Threat Signals at:
https://www.fortiguard.com/threat-signal-report/4335/apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.fortiguard.com/threat-signal-report/4339/new-log4j-vulnerability-cve-2021-45046-results-in-denial-of-service
https://www.fortiguard.com/threat-signal-report/4345/log4j-2-17-0-released-in-response-to-new-log4j-vulnerability-cve-2021-45105
https://www.fortiguard.com/threat-signal-report/4360/log4j-2-17-1-released-for-cve-2021-44832

**Announced**

On Dec 9, a 0-day was posted on Twitter with a PoC posted in GitHub. On Dec 10, several security-related websites picked up the vulnerability and released an article.

**Latest Developments**

Jun 27, 2022: Over 6 months later, stories of Log4j2 exploits continue to be published on near-daily basis and FortiGuard Labs continues to see active exploitation attempts. On a single day (Jun 14, 2022), FortiGuard IPS blocked over 50,000 exploits.

## Cyber Kill Chain

### Reconnaissance

**FortiDeceptor**
*Decoy VM 3.3+*
Detects activities related to the Log4j2 vulnerability

### Weaponization

### Delivery

**FortiClient**
*Vulnerability 2.087*
Detects presence of Log4j2 vulnerability on Linux machines

**FortiCWP**
*Vulnerability 21.3.0*
Protects CI/CD pipeline by detecting the presence of log4j2 vulnerability in container images

**FortiDevSec**
*Vulnerability 22.3*
Detects Log4j2 vulnerability in web application source code and packages through SCA scans, and earlier in the development lifecycle of the application on the CI/CD pipeline

### Exploitation

**FortiGate**
*IPS 19.231*
Blocks exploitation of the Log4j2 vulnerability

**FortiWeb**
*Web App Security 0.00308*
Blocks exploitation of the Log4j2 vulnerability

**FortiClient**
*Application Firewall 19.231*
Blocks exploitation of the Log4j2 vulnerability

**FortiSASE**
*IPS 19.231*
Blocks exploitation of the Log4j2 vulnerability

**FortiNDR**
*IPS 19.231*
Blocks exploitation of the Log4j2 vulnerability

**FortiADC**
*IPS 19.231*
Blocks exploitation of the Log4j2 vulnerability

*Web App Security 1.00030*
Blocks exploitation of the Log4j2 vulnerability

**FortiProxy**
*IPS 19.231*
Blocks exploitation of the Log4j2 vulnerability

### Installation

**FortiEDR**
*Post-Execution 5.0+*
Detects post-exploitation behavior associated with the Log4j2 vulnerability.

### C2

### Action

### Endpoint

## Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

**FortiEDR**

***Threat Hunting*** Version 5.0+
https://community.fortinet.com/t5/FortiEDR/Technical-Tip-How-FortiEDR-protects-against-the-exploitation-of/ta-p/201027

**FortiAnalyzer**

***Outbreak Detection*** Version 1.00041
https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00041

***Threat Hunting*** Version 6.4+
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-activities-related/ta-p/201026

**FortiSIEM**

***Threat Hunting*** Version 6.0+
https://community.fortinet.com/t5/FortiSIEM/Technical-Tip-How-to-use-FortiSIEM-to-detect-activities-related/ta-p/201082

### Additional Resources

| | |
|---|---|
| **CISA Gov** | https://www.cisa.gov/uscert/ncas/current-activity/2021/12/13/cisa-creates-webpage-apache-log4j-vulnerability-cve-2021-44228 |
| **US CERT** | https://www.cisa.gov/uscert/ncas/alerts/aa21-356a |
| **Apache** | https://logging.apache.org/log4j/2.x/security.html |
| **Threat Signal** | https://www.fortiguard.com/threat-signal-report/4335/apache-log4j-remote-code-execution-vulnerability-cve-2021-44228 |