



Apache 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	<p>The Log4j2 is a Java-based logging utility that is part of the Apache Software. For more details on the background please read Fortinet Blog: https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know</p> <p>To view, Fortinet products impacted by this vulnerability, refer to: https://www.fortiguard.com/psirt/FG-IR-21-245</p> <p>Technical information pertaining to each vulnerability, please refer to the FortiGuard Threat Signals at: https://www.fortiguard.com/threat-signal-report/4335</p> <p>https://www.fortiguard.com/threat-signal-report/4339</p> <p>https://www.fortiguard.com/threat-signal-report/4345</p> <p>https://www.fortiguard.com/threat-signal-report/4360</p>
Announced	Dec 9th: 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	<p>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.</p> <p>Feb 27, 2024: A new campaign conducted by the Lazarus Group is seen employing new DLang-based Remote Access Trojans (RATs) malware in the wild exploiting Log4j Vulnerability. https://www.fortiguard.com/outbreak-alert/lazarus-rat-attack</p>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

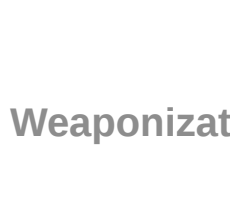
Detects activities related to the Log4j2 vulnerability



v5.0+

Decoy VM

Detects activities related to the Log4j2 vulnerability



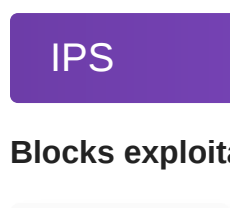
v5.0+

Weaponization

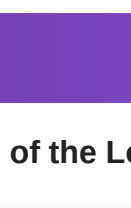
Delivery

Vulnerability

Detects presence of Log4j2 vulnerability



DB 2.087



DB 21.3.0

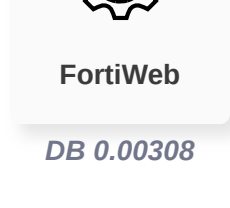


DB 22.3

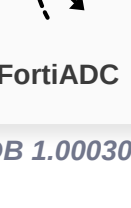
Exploitation

IPS

Blocks exploitation of the Log4j2 vulnerability



DB 19.231



DB 19.231



DB 19.231



DB 19.231



DB 19.231

Web App Security

Blocks exploitation of the Log4j2 vulnerability



DB 0.00308



DB 1.00030

Installation

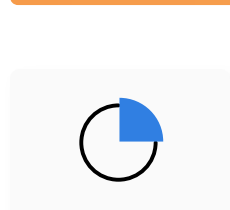
C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Threat Hunting



FortiClient



FortiAnalyzer

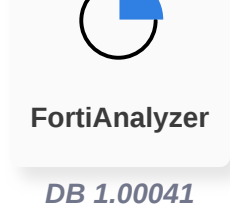


FortiSIEM

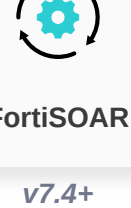


FortiEDR

IOC



FortiAnalyzer

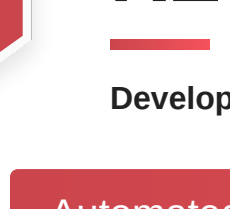


FortiSIEM

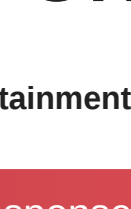


FortiSOCaaS

Outbreak Detection



DB 1.00041



FortiSOAR

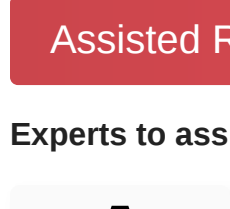
v7.4+

RESPOND

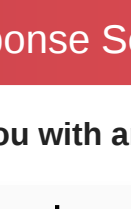
Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



FortiClient Forensics



FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.



Incident Response



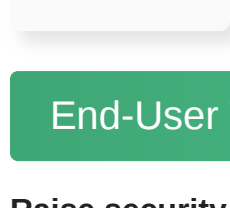
FortiRecon: ACI

RECOVER

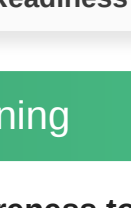
Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



NSE Training



Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.



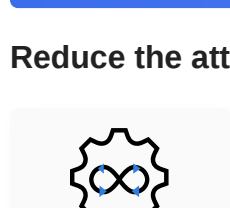
Security Awareness & Training

IDENTIFY

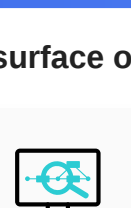
Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Security Rating



FortiDAST

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.



FortiDevSec



FortiEDR

Business Reputation

Know attackers next move to protect against your business branding.



FortiRecon: EASM

CISA	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
PSIRT	https://www.fortiguard.com/psirt/FG-IR-21-245
Threat Signal	https://www.fortiguard.com/threat-signal-report/4335

Learn more about [FortiGuard Outbreak Alerts](#)

