FORTINET

OUTBREAK ALERTS

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,CVE-2021-4104

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. 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

To view, Fortinet products impacted by this vulnerability, refer to:
https://www.fortiguard.com/psirt/FG-IR-21-245

Technical information pertaining to each vulnerability, please refer to the FortiGuard Threat Signals at:
https://www.fortiguard.com/threat-signal-report/4335
https://www.fortiguard.com/threat-signal-report/4339
https://www.fortiguard.com/threat-signal-report/4345
https://www.fortiguard.com/threat-signal-report/4360

Latest Developments

FortiGuard Labs continues to see active exploitation attempts and remain as one of the top routinely exploited vulnerability.

June 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

June 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.

December 10, 2021: Several security-related websites picked up the vulnerability and released an article.

December 9, 2021: A 0-day was posted on Twitter with a PoC posted in GitHub.

PROTECT

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

Reconnaissance

Lure

Detects activities related to the Log4j2 vulnerability

FortiDeceptor
v5.0+

Decoy VM

Detects activities related to the Log4j2 vulnerability

FortiDeceptor
v5.0+

Weaponization

Delivery

Vulnerability

Detects end-user devices running the vulnerable application.

FortiCWP
DB 21.3.0

FortiClient
DB 2.087

FortiDevSec
DB 22.3

Exploitation

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC
DB 19.231

FortiGate
DB 19.231

FortiNDR
DB 19.231

FortiProxy
DB 19.231

FortiSASE
DB 19.231

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiADC
DB 1.00030

FortiWeb
DB 0.00308

Installation

C2

Action

DETECT

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

IOC

FortiAnalyzer

FortiSOCaaS

FortiSIEM

FortiSOAR

Outbreak Detection

FortiAnalyzer
DB 1.00041

FortiSOAR
v7.4+

Threat Hunting

FortiAnalyzer

FortiClient

FortiEDR

FortiSIEM

Cloud Threat Detection

Fcnapplacework

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly 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 targeted 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

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

FortiRecon: EASM

Vulnerability Management

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

FortiClient

FortiDevSec

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: BP

Additional Resources

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
Threat Signal	https://www.fortiguard.com/threat-signal-report/4335
FortiGuard Labs Threat Research	https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know
PSIRT Blog	https://www.fortinet.com/blog/psirt-blogs/apache-log4j-vulnerability

Learn more about FortiGuard Outbreak Alerts

FORTINET