Log4J Vulnerabilities - Fortinet Resolutions (Updated to 12 Dec 2021)

The information provided below is referred from https://www.fortinet.com/blog/psirt-blogs/apache-log4j-vulnerability and https://www.fortiguard.com/psirt/FG IR-21-245?utm_source=blog&utm_campaign=blog.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 12, 2021

- **Threat Level**

  High

- **Response to Log4j**

FortiGuard Labs is aware of a remote code execution vulnerability in Apache Log4j. Log4j is a Java based logging audit framework within Apache. Apache Log4j2 2.14.1 and below are susceptible to a remote code execution vulnerability where a remote attacker can leverage this vulnerability to take full control of a vulnerable machine.

This vulnerability is also known as Log4shell and has the CVE assignment (CVE-2021-44228). FortiGuard Labs will be monitoring this issue for any further developments.

- **Affected Fortinet Products**

1. FortiAIOps – Fixed in version 1.0.2
2. FortiCASB – Fixed on 2021-12-10
3. FortiConverter Portal – Fixed on 2021-12-10
4. FortiCWP – Fixed on 2021-12-10
5. FortiEDR Cloud – Not exploitable. Additional precautionary mitigations put in place on 2021-12-10
6. FortiInsight – Not exploitable. Additional precautionary mitigations being investigated. FortiIsolator – Fix scheduled for version 2.3.4
7. FortiMonitor – Mitigations for NCM & Elastiflow available
8. FortiPortal – Fixed in 6.0.8 and 5.3.8
9. FortiSIEM – Mitigation available
10. ShieldX – Fix scheduled for versions 2.1 and 3.0 – ETA 2021/12/17

- **Fortinet Protection Products**

Protections are available across the whole Fortinet Security Fabric to help defend against this attack.

1. **FortiWeb/Fortigate IPS**

   Apply web application firewalling signatures and IPS to detect and prevent the vulnerability from being exploited.

2. **FortiGate Firewall**

   Employ firewall policy and microsegmentation to prevent authorized devices from communicating out to unauthorized resources.

3. **FortiEDR**

   Monitors and protects against payloads delivered by exploitation of the vulnerability.

4. **FortiCWP**

   Protects CI/CD pipeline and detects the presence of Log4j2 vulnerability in container images.

5. **IPS Signature Protection(FortiOS)**

   Fortinet has released IPS signature Apache.Log4j.Error.Log.Remote.Code.Execution, with VID 51006 to address this threat. This signature was initially released in IPS package (version 19.215). Please note that since this is an emergency release, the default action for this signature is set to pass. Please modify the action according to your need.

   As of IPS DB version 19.217 this signature was set to drop by default.

6. **IPS Signature Protection (FortiADC & FortiProxy)**

   FortiADC supports IPS signature to mitigate Log4j (version 19.215). FortiProxy supports IPS signature to mitigate Log4j (version 19.215).

7. **Web Application Firewall (FortiWeb & FortiWebCloud)**

   Web application signatures to prevent this vulnerability were added in database 0.00301 and have been updated in the latest release 0.00305 for additional coverage.