Log4J Vulnerabilities - Radware Resolutions (Updated to 20 Dec 2021)

The information provided below is referred from https://support.radware.com/app/answers/answer_view/a_id/1029752/~/cve-2021-44228%2C-a-critical-log4j-vulnerability, https://support.radware.com/app/answers/answer_view/a_id/1029778/related/1 and https://blog.radware.com/security/alert/2021/12/log4shell-critical-log4j-vulnerability/.

- **CVE Number**

  2021-44228

- **Discovery Date**

  No Information

- **Threat Level**

  Critical

- **Response to Log4j**

A critical vulnerability in Log4j package identified by CVE-2021-44228 with CVSS severity of 10, which is the highest score, has been publicly disclosed . The vulnerability may allow for remote code execution in impacted products. See also Apache note on this vulnerability

Radware is evaluating the impact of this vulnerability on its own product while at the same time providing protection in our cyber defense product and services allowing to block malicious actors from exploiting this vulnerability.
Radware's ERT researchers are continuing to research this vulnerability and its impact, and will update the guidance provided to customers when new information is available. Please make sure to check this advisory for ongoing updates.

- **Radware Mitigation & Protection**

Radware web application security solutions, AppWall and Cloud WAF Services, detected and blocked Log4Shell exploit attacks through web application parameters and HTTP header fields, from day one, as Server Side Request Forgeries.
Radware's researchers are developing signatures to be used to block these attacks.

Radware released a number of signatures to provide protection from this CVE as part of the latest Signature Update (13-Dec-21, 0009.0651.00).

1. HTTP-APACHE-LOG4j2-BODY-RCE (RWID 20276)
2. HTTP-APACHE-LOG4j2-URL1-RCE (RWID 20278)
3. HTTP-APACHE-LOG4j2-URL2-RCE (RWID 20280)
4. HTTP-APACHE-LOG4j2-URL3-RCE (RWID 20282)
5. HTTP-APACHE-LOG4j2-URL4-RCE (RWID 20284)
6. HTTP-APACHE-LOG4j2-BODY1-RCE (RWID 20286)

7. HTTP-APACHE-LOG4j2-BODY2-RCE (RWID 20288)
8. HTTP-APACHE-LOG4j2-BODY3-RCE (RWID 20290)