Log4J Vulnerabilities - Splunk Resolutions (Updated to 9 Dec 2021)

The information provided below is referred from https://docs.splunk.com/Documentation/ITSI/latest/Install/Addresslog4j and https://www.splunk.com/en_us/blog/security/log4shell-detecting-log4j-vulnerability-cve-2021-44228-continued.html.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 9, 2021

- **Threat Level**

High

- **Response to Log4j**

A serious vulnerability (CVE-2021-44228) in the popular open source Apache Log4j logging library poses a threat to thousands of applications and third-party services that leverage this library. Proof-of-Concept code demonstrates that a RCE (remote code execution) vulnerability can be exploited by the attacker inserting a specially crafted string that is then logged by Log4j. The attacker could then execute arbitrary code from an external source.

- **Affected Splunk Products**
    1. ITSI and ITE Work versions 4.11.0, 4.9.x (on-premises and cloud)ITSI 4.7.x (on premises and cloud)
    2. ITSI and ITE Work 4.10.x – Cloud-only versionITSI 4.5.x, 4.6.x, and 4.8.x – Cloud-only versions
    3. ITSI version 4.4.x (No longer supported as of October 22, 2021)

- **Splunk Workaround Solution**
    1. **Intrusion Detection Alerts**

        Make sure the IPS has updated the rules to detect and are indexing them in Splunk. In this case, it uses Suricata but this holds true for any IDS that has deployed signatures for this vulnerability. A quick search against that index will net you a place to start hunting for compromise
        index=suricata (“2021-44228” OR “Log4j” OR “Log4Shell”) | table _time, dest_ip, alert.signature, alert.signature_id

    2. **Splunk Recommendation**

        Patching is still your best bet to combat this vulnerability. If patching isn’t possible, implementing mitigation is the next best path to minimize the attack surface. SURGe is monitoring the evolution of this vulnerability and

will provide additional information as needed. Additionally, Splunk's Threat Research Team has been working hard to create some detections for ESCU as well as a SOAR playbook for automated response, which will be released as soon as possible.

For any other information to detect the Log4J Vulnerability, please go to:

https://www.splunk.com/en_us/blog/security/log4shell-detecting-log4j-vulnerability-cve-2021-44228-continued.html

For the detail workaround solution, please go:

https://docs.splunk.com/Documentation/ITSI/latest/Install/Addresslog4j