Log4Shell: Log4j Vulnerabilities Update

Executive Summary

This is an update around the threats and risks related to Log4j vulnerabilities, CVE-2021-44228 and CVE-2021-45046, as of December 17, 2021.

On December 15, 2021, a new vulnerability in Log4j was announced and cataloged as CVE-2021-45046. The vulnerability was analyzed and reported to invalidate logic-based (non-patching) mitigations against the unauthenticated remote code execution (RCE) vulnerability detailed in CVE-2021-44228 in Log4j < 2.15.0. Under certain conditions this vulnerability also results in a low impact denial of service (DoS) in Log4j 2.15.x was addressed in Log4j version 2.16, which was released 24 hours prior to the announcement of this vulnerability. As of December 17, further analysis showed an RCE vulnerability still existed even in Log4j version 2.15.x. CVE-2021-45046 was updated from a CVSS3.0 score of 3.7 (Low) to 9.0 (Critical) due to the bypass RCE vulnerabilities in version <=2.14.1 (as of December 15) and the recently discovered RCE in version <=2.15.x (December 17). Additionally, reports of exploitation of Log4j vulnerabilities by the Conti Ransomware group were published on December 17. This validates Optiv gTIC previous assessment from December 13 that ransomware groups will begin exploiting Log4j vulnerabilities within the next 7 days.

Updating to Log4j version 2.16.0 is highly recommended to address both CVE-2021-44228 and CVE-2021-45046. Optiv gTIC assesses with High Confidence that the release of Log4j 2.16.0, will significantly degrade and deter adversary attempts to compromise systems and servers via both vulnerabilities. It is Most Likely Log4j systems will continue to be targeted over the next 12 months by cyber adversaries to deliver follow-on malware like cryptocurrency miners, webshells, and disruptive/destructive payloads like ransomware and wiper malware.

Recommendations and Findings

Mitigation Recommendations

Optiv gTIC makes the following preventive and mitigation recommendations for the threats referenced in this report.

- Upgrade to Log4j 2.16.0.
- Maintain visibility and inventory of applications that depend on and use the Log4j library and ensure those applications are being updated.
- Log4j version 2.16.0, announced on the night of December 13, disables JNDI by default and removes support for Message Lookup. This release specifically addresses the RCE techniques and conditions (CVE-2021-45046) in Log4j <=2.15.x and the low-impact DoS vulnerability in Log4j 2.15.x.
Key Findings

- The initial NVD announcement of CVE-2021-45046 on December 15 failed to address the logic-based (non-patching and non-upgrade) mitigation RCE bypass conditions present in Log4j versions <=2.14.1. As of December 17, Log4j version 2.15.x was also analyzed and confirmed to have an RCE vulnerability.
- On December 17, the severity of CVE-2021-45046 is updated from Low (CVSS3.0 score 3.7) to Critical (CVSS3.0 score 9.0).
- Mature ransomware groups, like Conti Ransomware, are reported to be actively exploiting Log4j vulnerabilities as of December 17 and moving laterally to target VMWare vCenter. The Log4j vulnerabilities Likely include both CVE-2021-44228 and CVE-2021-45046.

Optiv gTIC Analysis and Comments

Scanning and exploitation attempts against both CVE-2021-44228 (Log4Shell) and CVE-2021-45046 will Most Likely continue over the next 12 months. This coincides with Optiv gTIC’s standing assessment that vulnerabilities in ubiquitous system continue to be scanned for and interrogated long after disclosures and patches are released. Optiv gTIC assesses with High Confidence that the release of Log4j 2.16.0 will significantly deter and degrade adversary attempts to achieve Initial Access via exploitation of CVE-2021-44228 (Log4Shell) and CVE-2021-45046; however, Optiv gTIC assesses with High Confidence that many organizations have not yet updated to either 2.15.x or 2.16.

Reports of ransomware infections and claims of state-sponsored scanning and exploitation attempts leveraging Log4Shell have been reported over the last 24 hours, including Conti Ransomware. This was a Likely scenario previously forecasted by Optiv gTIC on December 13th and within scope of predictable activity based off previous campaigns and exploitation trends. The relative ease of exploiting the Log4j vulnerabilities also makes it an attractive opportunity for cyber adversaries to achieve Initial Access.

Organizations are highly encouraged to continue to identify and address vulnerabilities in other critical software and services and leverage long-standing adversary and malware techniques for detection and prevention efforts beyond patching and workarounds. These measures constitute proper defense-in-depth plans.

Most Likely Course of Action*: Optiv gTIC assesses with High Confidence that CVE-2021-44228 and CVE-2021-45046 will be exploited by cyber threat actors over the next 12 months for Initial Access. Post-exploitation techniques will include ransomware and deployment of cryptocurrency miners on web and applications servers due to the ease of delivering and spreading cryptocurrency miners. Tools for further Persistence, Credential Harvesting, and Lateral Movement (e.g., Cobalt Strike, Mimikatz, PassTheHas, BloodHound/SharpHound, Ladon) are also Likely to accompany cyber-criminal compromises. It is Likely that Initial Access into organizations’ servers and networks via these vulnerabilities will be sold off to ransomware operators and affiliates on darkweb forums and markets to propagate more mature and advance ransomware programs.

Optiv gTIC continues to assess with High Confidence that Log4Shell will also be exploited to deliver webshells (Persistence, Collection, Exfiltration). Popular webshells known to be deployed in previously-observed campaigns include ChinaChopper, Awen, and AntSword. These webshells have been deployed using default settings based off observations and analysis of campaigns over the last 2 years and it is Likely default settings for webshells will be used in future compromises. Detection and prevention measures against these webshells is a key part of a proper defense-in-depth strategy which will protect organizations against attacks beyond Log4j vulnerability exploitation.

It is Very Likely that the disclosure of these Log4j vulnerabilities will have no impact on continued exploitation of vulnerabilities in other popular and ubiquitous software and services for Initial Access. These include Remote Desktop Protocol (RDP), Universal Plug and Play (UPnP), Microsoft Exchange, Oracle WebLogic, and Microsoft SQL Server. Disclosure of new critical vulnerabilities have been observed to result in an increase in attempts to exploit older vulnerabilities in similar products and services. Optiv gTIC assesses with High Confidence that an
increase in exploitation attempts of previously disclosed vulnerabilities in Apache Struts, Apache Tomcat, and Apache Solr will also increase over the next 30 days as a result of the Log4j vulnerability disclosures.

**Most Dangerous Course of Action**: Optiv gTIC assesses with High Confidence that Log4Shell will be exploited by robust and mature ransomware groups for Initial Access over the next 7 days. This estimate is based off previous observations of ransomware infections following critical vulnerability disclosures (0 – 10 days). Despite claims of state-sponsored scanning and exploitation, mass exploitation and compromise of Log4Shell by state-sponsored groups is overall Unlikely and will be restricted to businesses in key verticals. Optiv gTIC refrains from attribution at this time, as proper mitigation and preventive techniques and procedures take precedence to deter exploit attempts.

In the event of a state-sponsored attack, Optiv gTIC assesses with High Confidence that webshells will be deployed for Persistence, Collection, and Exfiltration. State-sponsored groups have also been known to deploy wiper malware and ransomware in limited campaigns and operations. Deployment of such malware by state-sponsored groups is Unlikely and will be extremely limited in scope.

A secondary/collateral threat is present in a scenario in which sophisticated adversaries begin targeting public collaborator servers for Reconnaissance is Unlikely but warrants consideration. The intent of this course of action will be to collect information on what software and components (including version) organizations are running within their environment. This information will enable efficient targeting by adversaries against organizations using tools and exploits specifically crafted or obtained for the vulnerabilities known to exist within that organization including, but not limited to, the Log4j vulnerabilities. Using private collaborator servers will reduce the risk of this attack vector.

*Most Likely Course of Action (MLCOA) – the expected and probable tactics, techniques, and actions carried out by a threat actor.

*Most Dangerous Course of Action (MDCOA) – tactics, techniques, or actions carried out or taken by an adversary that could result in a worst-case scenario outcome or impact, regardless of probability (MDCOA can also be referenced as MLCOAs if probability of occurrence is high).
Appendix A - References
