The Log Keeps Rolling On: Evaluating Log4j Developments and Defensive Requirements

blog.gigamon.com/2021/12/21/the-log-keeps-rolling-on-evaluating-log4j-developments-and-defensive-requirements/

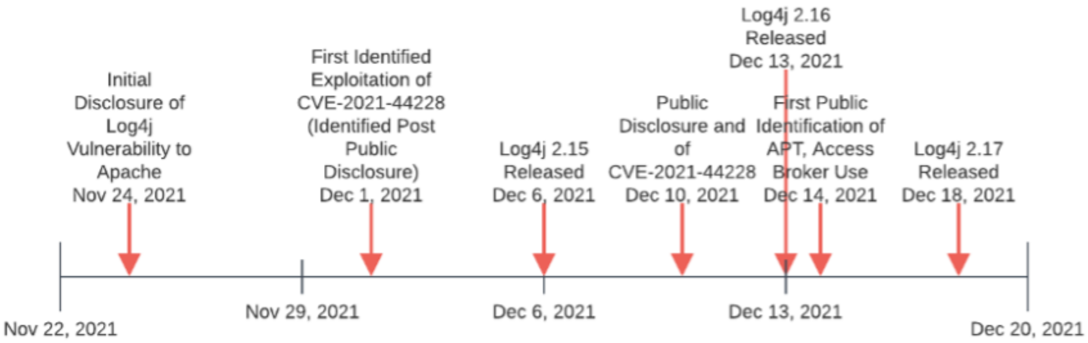
December 21, 2021

Threat Research / December 21, 2021

Joe Slowik &nbsp

Background

The information security world was turned upside down by the initial public disclosure of vulnerability CVE-2021-44228 in the Log4j application on December 10, 2021, colloquially referred to as “Log4Shell.” Subsequent investigation indicated initial exploitation of the Log4j application started in advance of public release, beginning as early as December 1 and proceeding through December 2. The following timeline provides an overview of events over the past few weeks.



Although covered by various entities near time of initial release, including a previous Gigamon article on network observations and defensive guidance, circumstances continue to evolve related to Log4j exploitation activity. This blog seeks to update earlier observations and provide extended guidance for defenders and network owners.

Trends Since Initial Release

Gigamon ATR observes several trends since initial disclosure of CVE-2021-44228:

1. Continued, high-volume scanning for CVE-2021-44228 by researchers and information security companies, as well as potential threat actors
2. Expansion of use beyond cryptocurrency miner and botnet installation to access development and ransomware-related operations

3. Increasing hype over the vulnerability as information concerning CVE-2021-44228 and other potential issues with Log4j spreads to more general audiences and non-technical decisionmakers

The combination of the above items results in a confusing and difficult landscape for security professionals and leaders. While weaponization of this vulnerability now extends to a broader set of more concerning adversaries (Item #2), continued scanning and related activity generate significant noise making identification of truly concerning exploitation attempts difficult (Item #1). With the addition of more widespread awareness of the problem (Item #3), security teams find themselves under increasing pressure to resolve issues in a chaotic, uncertain network environment.

To reduce confusion, the following represents a summary of key items of interest in Log4j activity since our initial publication on December 14.

State-Directed Exploitation

Reported initially by Microsoft on December 14 and extending to other security vendors shortly thereafter, state-directed exploitation (commonly referred to as “APT” activity) of Log4j now appears alongside more opportunistic, less-targeted use. For defenders, it is important to note that this date represents time of *disclosure* rather than time of *activity*. While specific information unfortunately remains unavailable, the exploitation window (starting potentially as early as December 1) means some adversaries (including potential state-nexus entities) had over a week to target this vulnerability before public disclosure. Security teams must take this into consideration when scoping investigations and framing forensic searches and queries for evidence of historical activity.

Gigamon ATR anticipates that state-directed (and other) adversaries will continue to leverage this vulnerability for both initial access to victim networks and lateral movement opportunities following a breach. As noted below, identifying and patching vulnerable services remains critical, but defenders must also be diligent in pursuing post-exploitation activity and similar behaviors as Log4j exploitation extends to increasingly capable and stealthy adversaries.

While the above activity is concerning, state-directed operations will likely remain focused on access development and information gathering for the foreseeable future. Organizations may be concerned that CVE-2021-44228 could be used for a potentially destructive cyber incident, such as the 2017 NotPetya event. While the possibility exists, Gigamon ATR assesses any such use would be incidental to the vulnerability in question and highly unlikely to spread in an uncontrolled fashion like NotPetya.

Although some social media reports exist claiming “wormable” malware linked to Log4j exploitation may exist (allowing for NotPetya-like scenarios), further analysis of known payloads indicates reliance on static lists of targets, use of a central resource for capability deployment, or other critical dependencies that remove true worm-like functionality.

Ultimately Log4j exploitation requires reference to a known, hosted resource to distribute whatever payload is retrieved and executed by the exploit, and this dependency presents a critical barrier to effective weaponization for widespread disruptive purposes. Log4j exploitation therefore just appears as “yet another” initial access mechanism that could be used for a variety of purposes, and does not appear especially capable or concerning from the standpoint of enabling a widespread disruptive cyber event.

Ransomware Operations

Likely more immediately critical to many organizations, ransomware-related entities appear to increasingly seek ways of using Log4j vulnerabilities to further operations. Starting on December 13, security firms identified possible attempts to use CVE-2021-44228 as part of ransomware distribution. These observations increased in subsequent days to include operations linked to entities working for or with ransomware distribution networks such as Conti.

Given the nature of the Log4j vulnerability, Gigamon ATR assesses that most ransomware operations will leverage this for developing initial access to targets instead of immediately deploying ransomware as part of exploitation. The general shift toward “big game” ransomware operations — encrypting entire networks instead of individual systems — means that Log4j-focused deployment would be limited in scope if used directly. This observation is reflected in Conti-related activity, where Log4j appears used as an access vector to then enable follow-on lateral movement within the network en route to mass distribution of ransomware in victim environments.

Log4j activity becomes concerning for ransomware defense though given the relative ease of exploitation and ability to do so external to victim networks. Given the division of labor in modern ransomware operations, where activities are divided between access brokers, exploitation teams, and actual ransomware deployment and negotiation entities, CVE-2021-44228 represents an amazing opportunity to rapidly expand into a variety of potential victim networks. Such access may not be immediately utilized, but instead sold to other entities who will then engage in more protracted infiltration of the victim network leading ultimately to ransomware deployment.

From a defender’s perspective, this activity is deeply concerning, but the sheer volume of activity may represent an opportunity as well. Simply put, the overwhelming number of potential new access points for ransomware operators may buy defenders time in identifying such intrusions before they are handed over to other entities for follow-on actions. As with the previous section, prioritizing post-exploitation behavior identification along with attack surface reduction will be key both in minimizing future exploitation and in identifying existing adversary intrusions.

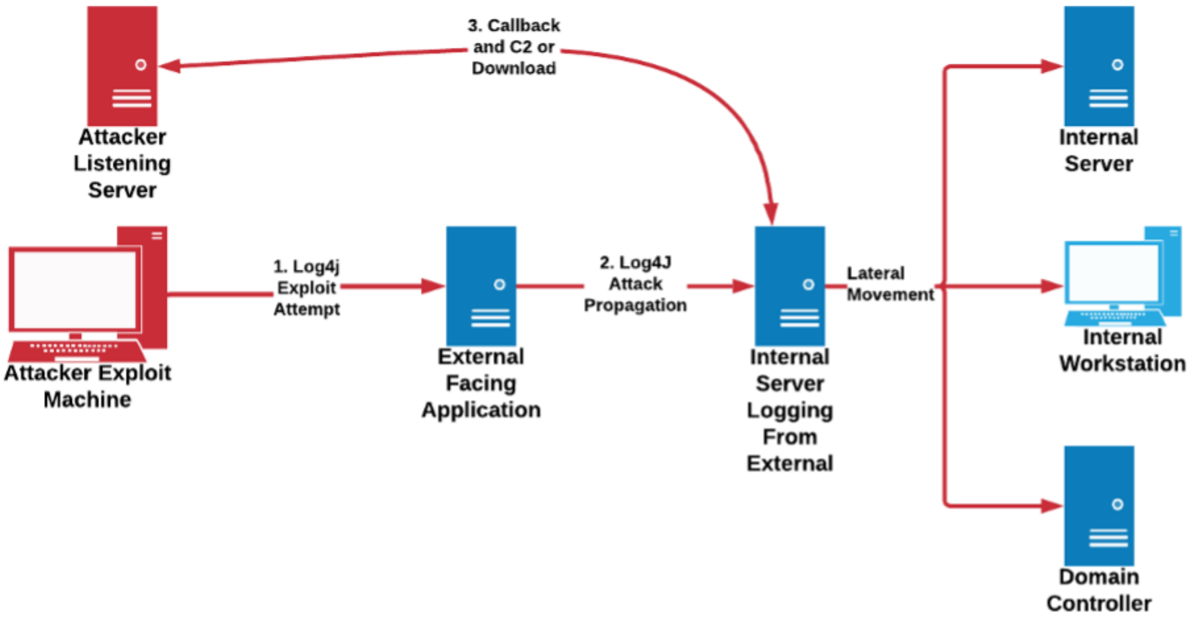
Opportunistic Scanning

While defenders cope with the above threats, various organizations continue to scan, and at times exploit, CVE-2021-44228 for multiple purposes. On the benign (but annoying) side, vulnerability researchers and trackers continue to scope the extent and prevalence of vulnerable systems for reporting and analysis purposes. While not leading to any malicious activity, the subsequent network traffic provides opportunities for more malicious entities to "hide" while also burning out front-line defenders responding to alerts and alarms. For example, Gigamon has observed hundreds of thousands of instances of CVE-2021-44228 exploitation activity in just a 24 hour period within a monitored environment — simply tracking scanning and exploitation attempts as individual alerts therefore becomes not just burdensome, but functionally impossible.

Gigamon ATR anticipates this activity will continue, albeit at a lower level following initial sweeps post-disclosure, for the foreseeable future. As a result, defensive postures seeking to identify and alert on *any* instance of CVE-2021-44228 exploitation or probing will likely result in significant "noise" for security operations. Defenders should therefore work to minimize rapid response to network traffic indicative of simply attempting Log4j exploitation. Instead, security personnel should focus on higher-fidelity analytic or composite alerting approaches linking such actions with higher-confidence observations, or focusing on post-exploit signs of activity across both host and network visibility.

Mitigations and Defenses

Defenders face a variety of problems related to CVE-2021-44228. One item that especially causes problems in scoping and understanding this vulnerability is its indirect nature. For example, a vulnerable server need not be directly accessible for exploitation to occur. A vulnerable system (e.g., a log aggregator or similar device) needs only to receive communications or parse information using a vulnerable service for successful exploitation to take place. As shown in the diagram below, an attacker initiates communication with an external-facing resource, but the actual attack payload is passed on to a remote logging system inside the victim network. This device actually processes the attack payload while parsing logs using the Log4j library, resulting in exploitation and subsequent communication to adversary infrastructure.


3. Callback and C2 or Download
Attacker Listening Server
Internal Server
1. Log4j Exploit Attempt
2. Log4J Attack Propagation
Lateral Movement
Internal Workstation
Attacker Exploit Machine
External Facing Application
Internal Server Logging From External
Domain Controller

Given this issue, simply prioritizing external-facing servers and applications for patching and defense is insufficient to address Log4j exploitation. Instead, defenders will need to identify subsequent communication links and dependencies to adequately reduce or eliminate attack surface. Defenders can take a variety of approaches to satisfy these needs, described in greater detail in the following sections.

Patch — Or Wait?

The first and most obvious solution to this issue is to patch vulnerable systems. However, this approach has several problems:

1. The sheer volume of scanning and exploitation activity means that many organizations are likely already facing a compromised environment from earlier operations, potentially even extending to prior public release of the CVE-2021-44228 patch
2. Patching Log4j instances directly only addresses code bases directly owned and maintained by the organization — multiple other vendors and application developers will need to patch their software to address nested use and system dependencies
3. Log4j patching itself has become confusing with the release of multiple patches since CVE-2021-44228 identification

Point #3 is especially vexing as organizations that rushed to apply patches as soon as possible find themselves having to do the same thing again with each subsequent release. In this case, it is worth noting that only CVE-2021-44228 allows for remote code execution (RCE) in *default configurations* of Log4j, and is addressed in version 2.15 and completely resolved in 2.16 by disabling JNDI. Subsequent releases address other security concerns, but either of lower potential value (e.g., denial of service conditions, the impact of which will vary depending on the application and business purpose) or in non-default configurations.

Asset owners and network defenders are strongly encouraged to read and understand release notes from the development team to understand what post-2.16 patches address. Depending on specific circumstances, organizations may need only be (immediately) concerned with the 2.16 update, and can de-emphasize subsequent patches if CVE-2021-44228 and similar worries are already addressed.

Point #2 is frustrating as it applies to systems and applications outside of the defender's hands. Multiple third-party software suites and applications leverage Log4j either directly or indirectly for functionality. Furthermore, the patching cycles of these organizations will vary depending upon the complexity of the software and the resources allocated to identifying dependencies then fixing them. The result is organizations will likely deal with vulnerable applications for many weeks — if not months — to come as third parties work to address this issue. Defenders and decisionmakers must understand these limitations and recognize that vulnerability to CVE-2021-44228 will likely persist for some time irrespective of the efforts of one's own team.

That leads to Point #1, where organizations must come to terms with the likelihood that they will face an intrusion due to this vulnerability — if they have not been breached already. This approach requires vectoring defensive resources and monitoring to post-exploitation activity and behaviors to ensure layered defense.

Post-Exploitation Monitoring

Most if not all organizations will find themselves in the position of either dealing with intrusions already achieved via CVE-2021-44228 exploitation, or unable to completely mitigate exposure from this attack vector for many weeks if not months. Defenders thus find themselves in the unfortunate position of dealing with intruders that have already succeeded in gaining access to networks. While less than desirable, this arguably reflects the reality network defenders already manage, only instead of a phishing message or other mechanism, personnel must deal with this (indirect) access route instead.

Defenders may find the exploitation route diagram above insightful for this activity as it reveals multiple opportunities for post-exploit detection. Assuming Log4j exploitation "lands" on a supporting, internal server instead of directly impacting the device receiving the initial network traffic, adversaries are placed in what initially appears to be an advantageous position as they have already breached the perimeter. For example, a potential intruder may blindly scan one's systems (or even just IP space) with an embedded exploit string. Even if none of these systems are directly vulnerable, or return a message such as an HTTP 404 response, any remote logging or forwarding may impact a vulnerable system linked to the external-facing service resulting in successful exploitation away from the network perimeter.

The above situation is challenging as it involves a web of dependencies, not all of which may be known or obvious to IT or security personnel. Yet defenders can look for the following general behaviors to identify post-exploitation activity:

1. Identifying anomalous or unexpected traffic from an *internal* server (especially a high-value device such as a logging or related system) to an external resource. Depending on an organization's tolerance and availability posture, such traffic could be blocked or filtered in addition to simply observed to preemptively reduce potential attack vectors.
2. Identifying remote authentication activity *from* an internal server *to* other hosts in the network instead of the reverse. This behavior reflects an adversary attempting to expand out of an initial "beachhead" in the network, but doing so by reversing the normal, expected flow of remote logon activity. Essentially, we expect clients to authenticate to servers, and not the opposite.
3. Monitoring for mass connectivity events, such as attempting to write to remote shares, scanning other systems, or attempting to remotely execute commands, from a server within the network, especially a system not tasked with active network management and administration tasks.

The above items all rely on a degree of asset identification and role understanding (e.g., differentiating a server from a client). But if an organization has already achieved some level of visibility and asset classification, powerful detection and defensive possibilities emerge for not only CVE-2021-44228 post-exploitation defense, but for entire categories of adversary tradecraft. If this type of defense and visibility is not already present within the defended network, asset owners should prioritize such efforts for future defensive planning and implementation.

In addition to the general traffic items above, available information thus far indicates after initial exploitation via CVE-2021-44228, adversaries revert to more typical, and well-known, intrusion techniques. For example, the Conti-related intrusions discussed previously may use CVE-2021-44228 as a novel form of initial access, but then use existing tradecraft compromising VMWare vCenter systems to achieve follow-on lateral movement and network exploitation.

Even more direct instances of post-exploitation activity, such as recently-identified use of Log4j exploitation to install Dridex or Meterpreter, requires follow-on functionality (either MSHTA in Windows environments or a Python script in Linux environments) for effectiveness. Monitoring for such activity across both host and network visibility, and especially chaining or linking events between such views, can identify such suspicious sequences of behavior for investigation and further action — but also reveals that adversaries remain committed to standard tradecraft following abuse of CVE-2021-44228.

Visibility and Vigilance

Overall, CVE-2021-44228 and subsequent Log4Shell activity shows the necessity of ensuring visibility of network traffic flows and host operations. Organizations with robust insights into these items have several opportunities to identify and then respond to intrusions leveraging even a nasty, widespread, trivially exploited vulnerability such as that in earlier versions of Log4j.

Where such visibility is lacking, network defenders and decision makers are at a loss for immediate events — but should use this long-running incident as an opportunity to influence and guide subsequent planning and investment. Essentially, CVE-2021-44228 is a terrible combination of accessibility and availability for a vulnerability, but it is not the first case of such activity, nor will it be the last. Furthermore, this vulnerability will likely persist as an issue for months to come as various vendors and software developers unwind and identify product dependencies and subsequently fix them.

By identifying appropriate lessons from this event and its weaponization by various threat actors, network defenders and other stakeholders can identify priorities for future security investments. This should start with ensuring that organizations possess the necessary visibility to even determine what is happening within the network, and being able to answer questions such as what actions are taking place not just at the external network boundary but within the organization's environment as well.

Conclusions

CVE-2021-44228 represents a very concerning security issue with immediate repercussions. There are a variety of steps that security teams must take in the near-term to address these challenges — but organizations and security leaders must also recognize that full response and mitigation of this vulnerability will likely require months of examination, patching, and continuous post-exploitation hunting to address.

The above observations and security advice represent general items applicable to all environments able to adequately view and aggressively query their network for signs of exploitation and follow-on activity. For organizations unable to implement this advice, this event should serve as a strong signal to begin implementing programs and procedures to improve insight into the defended environment so that administrators, defenders, and others can respond to and reduce the impact from the next major vulnerability to emerge.

Multiple stakeholders will be dealing with Log4j and its long tail of dependencies and installation instances through much of 2022. By continuously understanding how such a vulnerability is weaponized by attackers through intelligence and improving own-network visibility and monitoring through security operations, defenders can appropriately vector defenses to respond to these events and ensure that initial, potentially unavoidable breaches are quickly identified and removed.

Like most security operations, CVE-2021-44228 response will represent a test of long-term endurance and planning over months rather than a quickly realized sprint to security lasting a few days or weeks. The sooner network owners and defenders understand this approach, the better the overall community will be able to respond and begin mitigating this and similar, future events.

Featured Webinars

Hear from our experts on the latest trends and best practices to optimize your network visibility and analysis.

CONTINUE THE DISCUSSION

People are talking about this in the Gigamon Community's Network Detection & Response Group.

Share your thoughts today

RELATED CONTENT

REPORT

2022 Ransomware Defense Report

GET YOUR COPY >

WEBINAR

ThreatINSIGHT: Eliminating Adversaries' Dwell Time Advantage

WATCH ON DEMAND >

WEBINAR

Deep Dive INSIGHTS: Fighting Ransomware and Shifting Security Priorities

WATCH ON DEMAND >

OLDER ARTICLE
Revisiting Threat Models in the Cloud Era: A Webinar Series from ESG and Gigamon
NEWER ARTICLE
Customer-Based Orchestration Maximizes Choice and Eases Deployments

↑ TOP