How to Protect Your Organization from Log4j Exploitation

Well… here we go again with another major attack impacting our enterprise networks. This time, a critical, high impact, zero-day vulnerability (CVE 2021-44228) in the Apache Log4j library that is being actively exploited throughout the internet by cyber criminals and Nation State actors. Given the popularity of the Log4j software, it is estimated that this vulnerability could impact millions of systems. And because of the sheer number of vulnerable systems and the ease with which this vulnerability can be exploited, this is shaping up to be one of the biggest and potentially most damaging cyberattacks in history, and we still have two weeks left in 2021.

It is important to note that this attack is following a troubling trend – attackers are weaponizing newly disclosed vulnerabilities within hours of public disclosure of the issue. The race is on between attackers and defenders to get systems mitigated and patched before they are attacked.

Hopefully your organization has already mobilized against this very serious threat and is well on its way to mitigating the Log4j vulnerability within your environment. If you haven't yet mobilized, I'd recommend you make this your top priority. The question is, what should organizations be focusing on right now?

Step One: Identify Impacted Systems

Step one on the heels of any high impact vulnerability disclosure is to identify whether your systems are susceptible to the vulnerability. You will want to prioritize that investigation across your internet-facing systems first, as these are the systems that are easily scanned and exploited directly from the internet. Your second priority should be your systems that support your business-critical functions, including those systems that process and store sensitive data and Personally Identifiable Information (PII). Once those systems are validated as not vulnerable, you should turn your attention to your systems that connect directly to third-party partner systems. You'll want to ensure that if one of your partners is breached, attackers cannot move laterally from those external systems into yours. And finally, you will need to investigate systems not already covered by these initial priorities to identify any stragglers and close any gaps.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides some good guidance here on how to identify what systems are vulnerable. It also provides recommendations on how to mitigate vulnerable systems. There are multiple tools that have become available to help you identify these affected systems (including some great tools from Fidelis Security!). As a word of caution, you will want to ensure that those tools are from reputable and trusted sources. Attackers love to use these types of events to propagate malware through "free tools."

Step Two: Apply Mitigations

Step two is to apply mitigations. For applying mitigations, I would break this into two areas:

1. First is to make sure that your network and security stack (network and endpoint detection and response tools, firewalls, etc.) are updated to protect themselves against the vulnerability and to incorporate any vendor supplied Log4j/CVE 2021-44228

detection and blocking capabilities. If these tools are not adequately patched, they become yet another attack surface for the attacker. Provided they are not vulnerable, this detection and blocking capabilities help shield your vulnerable systems from exploitation while you are working to get systems-specific mitigations and patches in place.
2. Second is to apply mitigations to vulnerable systems. Use the same priorities discussed above for applying mitigations and patches to your systems – Internet facing systems, business critical systems, third party facing systems, and stragglers – and follow the recommendations and guidance of your vendors when applying patches and/or alternative mitigations. If you don't already have an accurate inventory of your systems that identifies your exposed systems, business critical systems, and systems that house your critical data, you will want to add this to your to-do list (after action report) so that you have this critical information readily available and are better prepared for future attacks.

Step Three: Assess Your Exposure

The Log4j vulnerability was publicly disclosed on 9 December 2021; however, there are reports of exploitation of the vulnerability beginning in early December. As a result, even if you quickly rolled out mitigations there is the potential that your systems were compromised prior to those mitigations being applied. As a first step in determining if your systems were impacted, I would recommend reviewing the logs associated with vulnerable systems (particularly internet facing systems) looking for signs of active exploitation of the vulnerability. Florian Roth's GitHub page, Log4j RCE Exploitation Detection, provides a good source of information for determining if the Log4j vulnerability was exploited on your systems.

While this is a good first step, I would recommend a more thorough "due diligence" assessment of impacted systems to ensure that the attackers have not compromised your systems. Some critical assessment capabilities include:

- Threat hunting tools
- Anomaly detection capabilities that can flag unusual user, system, and network behaviors.
- Retrospective analysis tools that can perform historical queries against communications metadata using Log4j Indicators of Compromise (IOCs)
- Deception capabilities that can readily identify lateral movement and other stealthy techniques and tactics used by the attackers.

Incident response tools to assist with "cleanup on aisle 9" will also be critical to determining if the Log4j vulnerability was exploited in one of your systems, if the attackers have further compromised the system, and/or if the attackers are attempting to compromise other systems.

As a final thought, I view where we are today as phase 1 of a multi-phased attack that I believe will continue to haunt us for the foreseeable future.

- Phase 1 involves the initial compromise of the system using the Log4j vulnerability to gain access to the system.
- Phase 2 will be efforts by the attackers to deploy additional exploitation tools on compromised system, escalate their privileges on the system, deploy persistence capabilities to allow them to regain entry into the system, and then cover their tracks to make it harder for the defenders to detect their presence.
- Phase 3 is when cyber-criminal groups will try to monetize these co-opted systems using ransomware, bitcoin mining, and other revenue generating attacks.

Based on this, I believe we have a small window of time to identify compromised systems and eject the attacker from our systems before significant damage is done.

Once again, Fidelis Security has some world class solutions in this space, and we stand by to assist our customers with mitigating the impacts of this attack as it evolves.