12/21/21 – Update

- We are happy to report that we have either already confirmed that we don't have exploitable installed versions of Log4J or have completed remediations based on the available information and vendor recommendations.
- While we believe that the iPipeline SaaS solutions are not exploitable using the Apache Log4J vulnerabilities, we will continue to monitor the situation through the holiday season and will respond should new critical vulnerabilities be disclosed or should our partners issue new guidance that requires immediate action. At this point we don't anticipate any additional changes related to this issue for the remainder of the year.
- We have not seen any indications of compromise associated with this vulnerability. We along with our MDR partner are continuing to closely monitor the situation.

12/20/21 – Update

- Following our vulnerability management process, iPipeline is continuing to closely monitor the evolving information regarding the Apache Log4J2 vulnerabilities and responding to them. The current evolving list of issues is below.

CVE-2021-44228 – A remote code execution vulnerability affecting Log4j versions from 2.0-beta9 to 2.14.1

CVE-2021-45046 – An information leak and remote code execution vulnerability affecting Log4j versions from 2.0-beta9 to 2.15.0, excluding 2.12.2

CVE-2021-45105 – A denial-of-service vulnerability affecting Log4j versions from 2.0-beta9 to 2.16.0

CVE-2021-4104 – An untrusted deserialization flaw affecting Log4j version 1.2

- We have either already confirmed that we don't have exploitable installed versions or are planning remediations based on the recently released information in an expedited manner.
- We will provide updates on this site.
- We have not seen any indications of compromise associated with this vulnerability. We along with our MDR partner are continuing to closely monitor the situation.

12/16/21 – Update

- We have not seen any indications of compromise associated with this vulnerability. We along with our MDR partner are continuing to closely monitor the situation.
- A 2nd vulnerability with Log4J was discovered on December 14th) (read more here). This one is rated as low risk and does not allow an attacker to gain access to computer systems. Nonetheless, we have evaluated and applied the fix where it could be done with minimal impact.

- We are continuing to remediate any remaining non-exploitable internal systems with urgency while ensuring that we do not negatively impact the availability of our services.

12/13/21 – iPipeline Response to the Log4J Vulnerability

On December 9, 2021, a zero-day vulnerability was reported in a software component (Log4j 2.x) that is widely used by many organizations (https://nvd.nist.gov/vuln/detail/CVE-2021-44228). The vulnerability can allow attackers to gain unfettered access to computer systems. We are not aware of any compromise or exploitation of this vulnerability within any iPipeline systems.

iPipeline has taken the following actions to address this serious vulnerability:

- We have audited our code repositories, 3rd party software, and running instances to identify any vulnerable installations of Log4J.
- Any known exploitable instances of Log4J have at this point been mitigated.
- Our MDR (Managed Detection and Response) partner has developed a prevention policy that will help identify any exploitation attempts. They are on heightened alert for any abnormal activity.
- We continue to closely monitor the situation both internally and with our partners.