Eric Cammarata

Minitab Interview Assignment

On December 9, 2021, security researchers discovered a 0-day vulnerability in a popular Java logging framework, Log4j. For this assignment, imagine you were working as a security engineer at a software company on the day that it was discovered, and answer the following questions:

1. **What source or feed would you have likely heard of this vulnerability?**

I would have likely first heard of this vulnerability through a news outlet. I actively try to stay updated on current events involving cybersecurity by reading news articles every day. Some sites that I frequently access for cybersecurity news include: cyware.com, thehackernews.com, and wired.com. All those mentioned sites provide great coverage of current events relating to cybersecurity. As I previously mentioned, I usually read a couple articles each day to stay updated.

1. **What would your immediate action be upon discovering the vulnerability?**

Upon first discovering the Log4j vulnerability, my immediate action would be figuring out if this vulnerability affects my software company. I would immediately set up meetings with our software engineers and developers to discuss with them whether any of our Java written software products utilize the Apache Log4j logging library. I also would have them review all our software product code to properly identify if any of our products contain the vulnerability or not.

1. **Describe the vulnerability at a high level, and what sort of systems would be impacted.**

Log4j is a logging library for Java that is open source and widely used by business and web portals globally. It is used to log all sorts of activity and event data. Back in December 2021, it was discovered that a remote hacker would potentially be able to execute malicious code. This could allow them to steal data or perform denial of service attacks on targeted servers. Any software or service that utilized the Log4j logging library would be vulnerable. As I previously mentioned, it was being used widely around the world by many businesses and websites, therefore, they were all at risk of having this vulnerability exploited.

1. **What methods would you use to determine whether any of the products or services your company offers are affected?**

I would begin by working with the company’s software engineers and developers to determine if any of our Java written software products or services utilize the Log4j logging library. I would have them double check and review the code of our software products. Finally, as a security engineer, I would work with my team to perform penetration testing on our products to see if we can identify the vulnerability. The cybersecurity technology company Crowdstrike developed a free Log4j search tool to help organizations identify the vulnerability by scanning given sets of directories for known checksums for Log4j. My team would utilize this tool to search our products and services for the vulnerability. Any products that are Identified to contain this vulnerability will be reported and logged, and mitigation measures will be looked into.

1. **You discover that your company hosts a cloud product that contains the vulnerability. What remediation steps would you recommend?**

After discovering this, I would recommend the following:

* First isolating the cloud product from the network
* Installing the latest version of Apache Log4j (Apache patched this vulnerability about a week after its discovery)
* Install or update security measures on the cloud servers to detect the launch of any malicious code so it can be stopped.

After these steps are taken, I would recommend that the cloud platform be reconnected to the network and receive continued monitoring for any potential exploits. Users of the company's cloud product should also receive notice that the company has taken measures to protect them from this vulnerability and is continuing to monitor the situation.

1. **Going forward, what steps would you recommend to detect and prevent vulnerabilities such as this one from affecting the company’s products?**

Going forward, I would recommend continuous monitoring for any exploits and to make sure that any security software used is regularly updated. On top of that I would recommend penetration testing on all company products regularly to test for new vulnerabilities.