Log4j vulnerability alarming news for digital service builders and consumers

10 January 2022, 01:00

Tatiana Galibus

The end of December 2021 brought alarming news for digital service companies all over the world due to the discovery of a critical vulnerability in the Apache Log4j library. This open-source library is broadly used for logging security and performance information. That is why Log4j is a common part of consumer and enterprise services and applications. Sadly, it also affects manufacturing companies, as it is widely used in operational technology products.

Who is affected?

Any application and service using the Java logging library, Apache Log4j (CVE-2021-44228), between versions 2.0 and 2.15. This includes services as **Atlassian, Amazon, Microsoft Azure, Cisco, Fortinet, Oracle, Red Hat, Splunk, Soft, and VMware**.

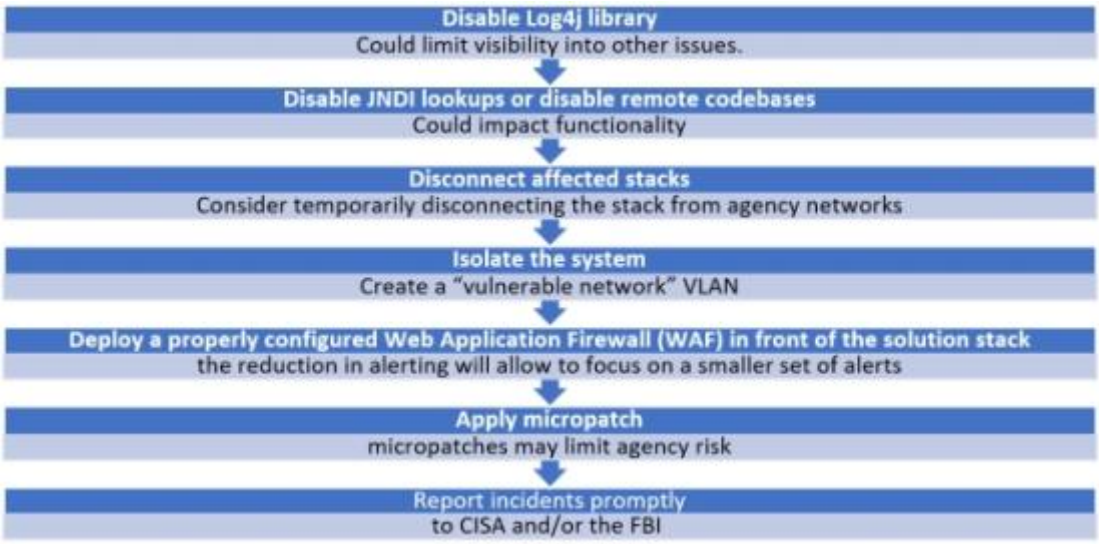
Therefore, it is present in the majority of popular apps and websites, and hundreds of millions of devices accessing these services around the world are potentially exposed to the vulnerability.

What is the impact?

Being a zero-day vulnerability, Log4j allows adversaries to execute any code remotely, whether over LAN, WAN, or the internet. **Besides, it can be exploited in a short time frame**. The vulnerability affects **log messages processing**. A threat actor can cause the system to load external code just by sending specially crafted message (remote command execution). The most alarming truth about such attacks is that it may take years to address this vulnerability for smaller companies while hackers are already looking constantly for the ways to weaponise and exploit it.

The most alarming truth about such attacks is that it may take years to address this vulnerability for smaller companies, while hackers are looking constantly for ways to weaponise and exploit it. Very soon, they might use it for more sophisticated attacks to get a bigger gain, so in the nearest future it can turn into a ticking bomb.

What is the mitigation?



Reports can be submitted here. Check this page for updates on mitigations.

What's next?

"What I'm most concerned about is the school districts, the hospitals, the places where there's a single IT person who does security who doesn't have time or the security budget or tooling," said Katie Nickels, Director of Intelligence at cybersecurity firm Red Canary. *"Those are the organisations I'm most worried about -- small organisations with small security budgets."*

Unfortunately, dealing with such supply chain vulnerabilities often engages third-party security scans and incident detection skills. How to efficiently raise awareness and cope with Log4j or other critical vulnerability in the software you are using on a daily basis? The best way is to learn how to protect yourself and react smartly! Sirris and Agoria provide such opportunity: learn about cybersecurity in an applied pragmatic way in a range of our masterclasses! All trainings are subsidised by VLAIO, so companies from Flanders will pay only 30 percent.

Authors

Tatiana Galibus