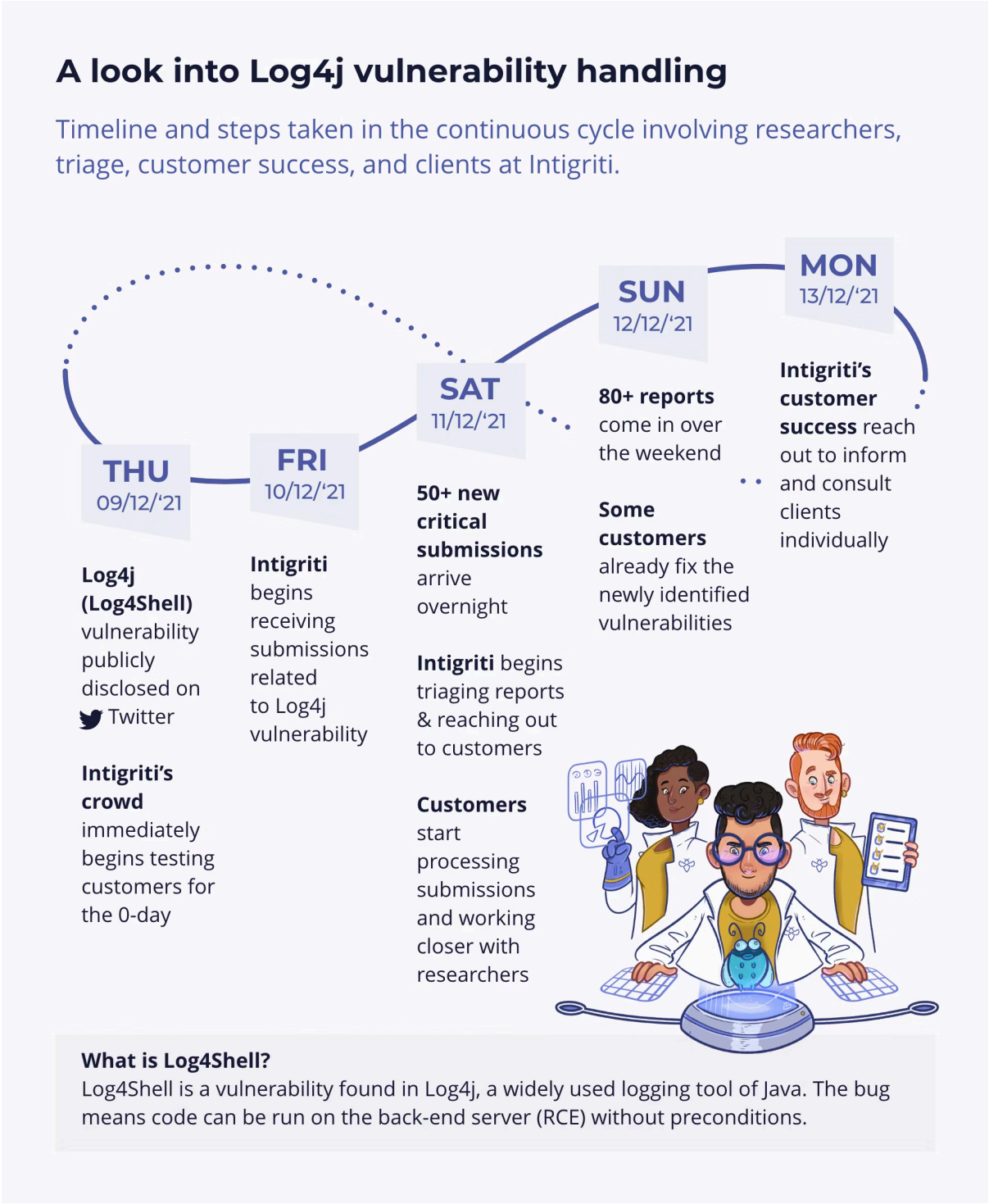
How Intigriti responded to the Log4j vulnerability

BY ANNA HAMMOND · DECEMBER 14, 2021 · LAST UPDATED ON MARCH 6, 2025

*In this article, we'll demonstrate **how crowd security platforms** give organizations additional support and assurance when a public zero-day vulnerability disclosure, such as Log4Shell (the Log4j vulnerability), happens.*

Last week, a zero-day vulnerability (Log4shell) was publicly disclosed in the widely-used Java-based logging library, **Log4j.** As a leading ethical hacking and bug bounty platform, testing in an agile way and against ever-evolving security vulnerabilities isn't unusual. However, given the severity of the vulnerability and public nature of the disclosure, our team knew that we needed to move fast to ensure our customers' infrastructures weren't exposed.

Upon hearing the news, Intigriti's security analysts flew straight into action. Over the course of the weekend, our analysts took triaging to new heights by assessing 80 new reports directly connected to the zero-day vulnerability—most of which were of critical to exceptional severity. Below, we go into more detail about the steps we took to help our customers bring patches into place as quickly as possible.



How Intigriti responded to the Log4j vulnerability public disclosure

The Log4j vulnerability: What happened?

On December 9th, 2021, the most serious vulnerability was disclosed on the Internet since the Heartbleed and Shellshock bugs, under CVE-2021-44228. The Log4j vulnerability is listed as a critical RCE, meaning an attacker can execute malicious code on a remote server. Due to the widespread use of Java and Log4j, the vulnerability could impact a significant portion of infrastructure worldwide.

A vast amount of effort went into mapping out the attack surface for this vulnerability by the ethical hacker. While it's straightforward to map out internally developed applications with the affected versions

of Log4j, many companies also run third-party software (or even software or hardware appliances running a covert vulnerable Log4j library), for which companies are dependent on the vendors. This makes the vulnerability particularly difficult to track.

What should your organization do now to protect its systems?

A message to Intigriti clients

Speaking directly to clients, Intigriti's CEO, Stijn Jans, says:

"Firstly, we would like to assure you that our platform is not developed upon Java technology and internal research has shown that we are not impacted by the log4j vulnerability. Secondly, many of you have been working round the clock to get patches in place. Once you have completed this activity, please do utilize your program at Intigriti to encourage researchers to check fixes and all assets by putting a clear briefing in your program that sets expectations for both you and the researchers.

Your success manager can assist you with the right wording that fits with your situation to update your program. Finally, should you need any additional support you feel Intigriti can assist with, please do not hesitate to reach out to the team. This has been a very tough week for many of us and we want you to know we are here to help."

Non-clients needing advice

If you're not set up with a bug bounty program, schedule a conversation with our security experts today to discuss how you can transition from occasional spot-check testing to continuous testing.

Crowd security platforms & new security vulnerabilities: How they help

When a new security vulnerability emerges that applies to many applications worldwide, one of the advantages of working with a crowd security platform is that you're likely to know whether your organization is affected extremely quickly. This is because researchers on the platform are quick to copy the technique that was publicly shared in a bid to be the first to disclose the same issue to your company, and therefore score a bounty. This is a real comfort to organizations in a time when malicious actors may be doing the same.

At Intigriti, the support in times of a public disclosure doesn't stop at the immediate activation from the crowd. Account management, customer success, triage, and technical support are included in every subscription—and as already mentioned, Intigriti's team dedicated additional hours in response to Log4j to ensure companies had the relevant support and information to minimize their risk.

How traditional testing methods fall short in these instances

Events such as the Log4j public disclosure shine a light on why continuous security testing is paramount for any digital organization operating today. Despite the emergence of this new zero-day vulnerability, pentesters aren't responsible for alerting previous customers to the information or performing additional checks. Consequently, organizations may not become aware they're at risk of this critical vulnerability until their next pentest.

In the case of the Log4j bug, testing against it alone is particularly difficult because it isn't always clearcut where Log4j is used (within their attack surface, third-party vendors, applicants, or cloud software, for example) or how it is used.

By having a bug bounty program, however, organizations have the assurance that they are continuously being tested against for the latest cyber threats by thousands of security experts.

Unlike pentests, organizations pay only for genuine, unique, and in-scope vulnerability reports rather than the time spent security testing. How much a company pays out for a report of this severity is up to them—but the potential expense and brand damage of a malicious hacker finding the vulnerability first is significantly less costly than a bounty fee.

Should organizations pay bug bounties for zero-days?

Most Intigriti customers have a 14-day cooldown period for zero-day vulnerabilities. This means that submissions sent through the platform during this timeframe do not automatically qualify for a bounty. It allows your team to assess the situation internally before including the issue in your bug bounty program. Researchers are still able to submit the vulnerability to your program and may receive a bonus at your discretion.

Get in touch

Our team is ready to show you how bug bounty can help your business stay ahead and fix the latest security vulnerabilities through bug bounty.

Contact us today.

Benefits of crowd-sourced bug bounty:

- Continuous and agile security testing through the power of the crowd
- Keep up with the latest vulnerabilities and security threats
- Reduce the risk of losses from a cyberattack
- Increased reputation and trustworthiness as data protectors

Intigriti's platform at a glance:

- 40,000+ creative and ethically-motivated security researchers
- Companies of all sizes trust our platform to leverage the creativity of the crowd
- Proactive and responsive triage team for added ease-of-mind
- Exceptional customer support throughout the setup process and post-launch

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com