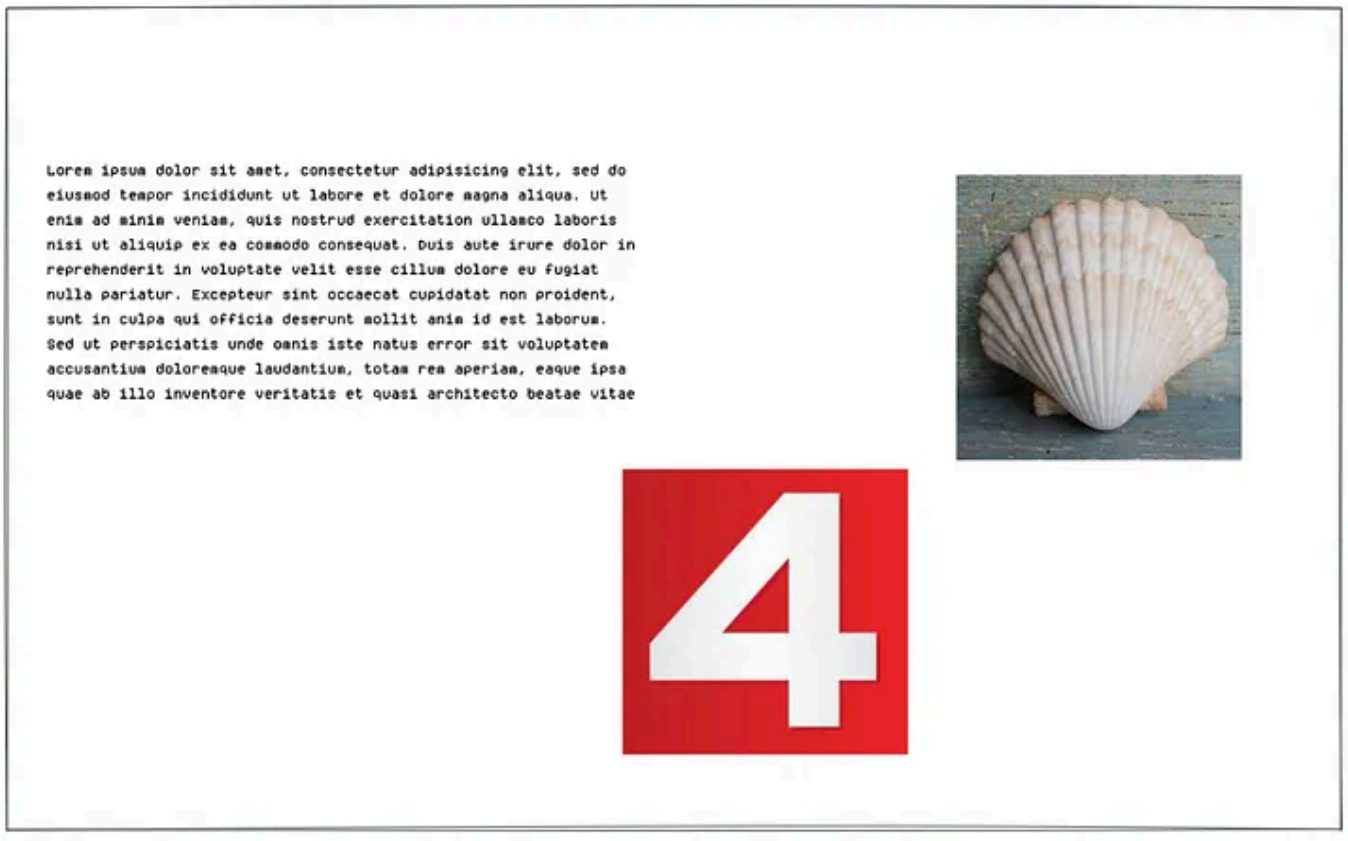
Member-only story

Text4Shell Exploit Walkthrough

The “4Shell” Sequel Continues???

Alex Rodriguez · Follow

Published in Geek Culture · 4 min read · Oct 24, 2022



Another vulnerability exploiting insecure string substitution in the Java programming language has been found. This time **the vulnerability impacts Apache’s Commons Text library** which provides APIs for string manipulation. The vulnerability is being tracked as CVE-2022–42889 and has a CVSS critical rating of 9.8. According to researchers, the likelihood of exploitation is much lower than that of the Log4Shell vulnerability because the library must be used in a specific way in order for an attacker to exploit the flaw. With that said, the vulnerability still allows for remote command execution, hence its severity score. In this blog post, I’ll help you setup a Java app vulnerable to Text4Shell and exploit it. Let’s do this!

> *NOTE: to better understand this exploit, I recommend checking out my Log4Shell exploit walkthrough blog post and the references section.*

Setup

Requirements

- Linux Virtual Machine (preferably Ubuntu/Debian based)
- wget, tar, and git should be installed

The following command downloads Java 19.0.1 and Maven 3.8.6 and places them in the `/opt` directory, adds the Java and Maven binary paths to your shell’s `$PATH` variable, and then sources `~/.profile`. Copy the…



Written by Alex Rodriguez

Follow

2.1K Followers · Writer for Geek Culture

I am an Offensive Security Engineer @ Amazon who writes about cybersecurity and anything related to technology. Opinions are my own.