Using Components With Known Vulnerabilities

1 min

Software often uses pre-existing components like modules or libraries. Components are helpful and sometimes a practical requirement, but you need to take care when using them; a component with vulnerabilities can pass those vulnerabilities onto software that uses them.

One example of a vulnerable component's impact is the Log4Shell

Preview: Docs Loading link description

vulnerability

. Log4Shell was an arbitrary-code-execution vulnerability in the Log4j logging framework for Java, which was used for everything from enterprise cloud software to Minecraft. Upon public disclosure, it was given a 10/10 severity score.

Part of the reason Log4Shell was such a serious vulnerability is that it was not known to the public. However, it became known in 2021, and as of 2024, there are still vulnerable systems. While zero-day vulnerabilities capture media coverage, most vulnerabilities that get exploited "in the wild" are publicly known vulnerabilities with patches available.

While it isn't possible to know definitively that a component doesn't have vulnerabilities, we can and should ensure that we're not using ones we know have vulnerabilities.