1100 - Exploiting Continuous Integration (CI) and Automated Build systems

Sunday at 11:00 in Track 3
45 minutes | Demo, Tool, Exploit
spaceB0x*Sr. Security Engineer at LeanKit Inc.*

Continuous Integration (CI) systems and similar architecture has taken new direction, especially in the last few years. Automating code builds, tests, and deployments is helping hordes of developers release code, and is saving companies a great amount of time and resources. But at what cost? The sudden and strong demand for these systems have created some widely adopted practices that have large security implications, especially if these systems are hosted internally. I have developed a tool that will help automate some offensive testing against certain popular CI build systems. There has been a large adoption of initiating these builds through web hooks of various kinds, especially changes to public facing code repositories. I will start with a brief overview of some of the more popular CI tools and how they are being used in many organizations. This is good information for understanding, at a high level, the purpose of these systems as well as some security benefits that they can provide. From there we will dive into specific examples of how these different CI implementations have created vulnerabilities (in one case to a CI vendor themselves). Last we will explore the tool, its purpose, and a demonstration of its use. This tool takes advantage of the configurations of various components of the build chain to look for vulnerabilities. It then has the capability to exploit, persist access, command and control vulnerable build containers. Most of the demonstration will revolve around specific CI products and repositories, however the concepts are applicable across most build systems. The goal here is to encourage further exploration of these exploitation concepts. The tool is built "modularly" to facilitate this. If you are new to CI and automated build systems, or if you have been doing it for years, this talk and tool will help you to better secure your architecture
spaceB0x
spaceB0x is extremely dedicated to his work in information security. He is the Sr. Security Engineer at a software company called LeanKit. He likes, and occasionally succeeds at, security dev-opsing, web application and network penetration testing, and some other security things. He has written tools for secure key management within automation infrastructures, capturing netflow data, and pwning automated build systems. He loves the hacker community, learning new things, and exploring new ideas.

@spaceB0xx
Website: www.untamedtheory.com

#defcon25/by_track/track3/sunday #defcon25/By_Day/_Sunday