MAJOR FLAW IN KUBERNETES COULD LEAD TO PRIVILEGE ESCALATION

In this Run and Reinvent podcast, I chat with Rick Bosworth, director of solutions marketing here at BMC, about the recent Kubernetes vulnerability and its potential impact on the enterprise. Below is a condensed transcript of our talk.

Jill Perez: To set the stage, for those that don't know, what is Kubernetes?

Rick Bosworth: Kubernetes is an open-source container orchestration platform. And is the market leader for container orchestration.

Jill: What exactly was the big security news on Kubernetes?

Rick: In December 2018, ZDNet published an article that made the rounds here within BMC. And this article described a major security flaw within Kubernetes. This vulnerability is affectionately named, CVE-2018-1002105, or simply, the Kubernetes privilege escalation flaw. So, it rates as CVSS score of 9.8. And, by comparison, everybody seems to be familiar with WannaCry. WannaCry was an 8.1.

Jill: What does CVSS stand for?

Rick: Common Vulnerability Security Score. It's a way of measuring the relative severity of vulnerabilities to each other. Kind of like we do earthquakes on a scale of one to 10. So, this means that a 9.8 is pretty much earth-shattering.

Jill: In a nutshell then, what is the actual vulnerability?

Rick: I'll try not to geek out here. So, the privilege escalation flaw enables bad guys to grab – or girls – grab full administrative control of any compute resource run in a Kubernetes' cluster. So, this is bad, bad, hair-on-fire bad. So, there's a good deal of technical detail about this vulnerability on the web and I'll not attempt to parse that here. You can pay me later, but suffice to say, anyone who is aware of this vulnerability, and now we must assume that everyone is because it's been reported on, can become admin of your Kubernetes servers.

They can kill containers, start new processes, and install malware like that which is used to mine Bitcoin and other cryptocurrencies. Now, for the uninitiated, so-called cryptojacking is computationally intensive and therefore, very costly. But for the pirates, it doesn't cost them anything because you would be paying for them, for the compute time. So, you'll be paying for Bitcoin's pirating of your infrastructure.

But that's just one example. You could think bigger picture. They could delete your production applications, kill them, hold them for hostage, effectively bring your business to its knees.

Jill: Who would be affected and what exactly would the solution be?

Rick: Anyone running Kubernetes version 1.0 – still 1.9 is affected. Patched versions are available in Kubernetes 1.10 and higher. So, the solution is – I'm afraid to say, and this is going to be a bitter-tasting pill. Customers absolutely have to upgrade their Kubernetes environments. So, as disruptive as that sounds, and I can imagine a bunch of IT people groaning right now. It pales in comparison to the threat that your business faces right now. Bringing your business down or allowing, worse yet, just allowing bad actors to sneak in through the open front door and just hang out for a while undetected and do who knows what later.

Jill: How would someone figure out if their business is exposed?

Rick: We became aware of the vulnerability on December 3rd. And as I mentioned, the emails were making the rounds and our Cloud Operations team was talking with our security team. Like many in the industry, we were hustling trying to get our arms around this and figure out the implications to us and implement a remedial plan of action.

So, on December 6th, we released a policy, a security and compliance policy, for TrueSight Cloud Security, which will automate a security check of the Kubernetes deployment and flag any noncompliant versions. So, typically we talk about TrueSight Cloud Security as automated find and fix, but here it's find and flag because really the only fix is to upgrade your Kubernetes deployment. But with it a customer's security and compliance team could shut down the vulnerable Kubernetes environment and, as previously mentioned, the only solution is to upgrade Kubernetes to 1.10, 11, or higher.