THE COUNTDOWN TO DOOMSDAY HAS BEGUN, ARE YOU READY?

The Countdown has begun

To be specific, the docker vulnerability dubbed Doomsday was exposed to the world just over 30 days ago. It's a bad one, and has the potential to spread to your entire container ecosystem. If you follow the cyber security industry, you know that on average we start to see exploits and hacks showing up within 30 days. A patch has been available for several weeks now, are you ready? This is a vulnerability that allows malicious code to jump from container to container until it spreads, undetected throughout your entire system.

The closest (recent) example we had was WannaCry back in 2017. Within a single day, the code jumped from one system to more than 230,000, encrypting hard drives as it went. Let me ask you, if WannaCry did not show itself so quickly (encrypting your hard drive and demanding a ransom), how far would it have spread?

The need to take action

Why take action? To start, you must understand the difference between the attack vector (or hack) and the payload (or malicious code). With Doomsday, we know the attack vector (a specific vulnerability in docker), but the payload could potentially be anything. I'm sure there are many

malicious actors right now utilizing that attack vector to inject MANY different kinds of payloads into containers. Some may be injecting key loggers, scanning for databases, or opening a back door into your network. How damaging and widespread do you think WannaCry would have been if it's payload was a silent piece of code that did not immediately expose itself, but went on for days/weeks/months logging your keystrokes and reporting your secrets home? This is the situation that's about to hit the world.

A doomsday hack starts by either download loading a base container that has malicious code or utilizing a 3rd party library inside your container that has been exposed. Unfortunately, sysadmins frequently utilize the first base container they find, without really inspecting the source. Likewise, developers use 3rd party libraries to help accelerate their development velocity. Neither is uncommon at all, and both have the ability to kick off this scenario in your environment.

How BMC can help

There is a bit of good news though, at BMC, we have decades of experience in automation that addresses problems just like this. Anybody that was using Truesight Cloud Security (TSCS) had zero concerns. Part of the docker best practices and CIS standards (which TSCS enforces) would have prevented the spread of code past the initial infected container, limiting the impact to just one. Truesight Vulnerability Manager was designed to help IT Ops and Security rapidly assess how and where the vulnerabilities exist, then integrate with an automation engine like Truesight Server Automation to automate the resolution of these issues.

Automation is the best weapon you have against the ticking clock. When hackers are exploiting new vulnerabilities within weeks, yet the industry on average takes 84 days to patch, we have a huge gap in our security practices. Let us help you close that gap and protect your environment.

Contact our sales department for help