FIND AND FIX DOCKER DOOMSDAY WITH BMC

Benjamin Franklin once said that “an ounce of prevention is worth a pound of cure.”

That quote is true today just like it was in the 1700’s, and while he was actually talking about fire safety (some believe he was referring to staying healthy – not true), Mr. Franklin could just as easily have been talking about protecting against security vulnerabilities, including a new and very dangerous one, Docker Doomsday.

What is Docker Doomsday?

The Docker Doomsday vulnerability affects almost any organization using Docker and containers. Here’s a quick look at what it does. First, an attacker infects a container with a malicious program. The malicious code exploits a flaw in runc, which is the container runtime utility for Docker and Kubernetes.

Next, the malicious code breaks out and infects the entire container host, and spreads to potentially thousands of other containers running on that host. This is a Doomsday scenario because the attack can ultimately affect many interconnected, production systems.

How bad is Docker Doomsday?

Well, it’s CVE 2019-5736 and has an overall Common Vulnerability Scoring System (CVSS) value of 8.6, that’s on a scale of 1-10 where 10 is as bad as it gets. Another perspective comes from RedHat.

They classified it as "Important Impact", a category reserved for vulnerabilities that can lead to unauthorized access to sensitive data, or a denial of service.

How to Solve for Docker Doomsday

Now the good news. Since the leading security vulnerability scanners (such as Qualys and Nessus) can find Docker Doomsday, you can run a scan and automatically import the vulnerability data into TrueSight Vulnerability Management. There you can analyze it and leverage its integration with TrueSight Server Automation to fix it, either on-premises or in the cloud. If you want to go one step further, use BMC Helix Discovery to find "blind spots" (cloud-based Docker instances that the scanners missed) to obtain a complete picture of where Docker Doomsday exists.

If you are in Cloud Operations and use BMC Helix Cloud Security, you can scan your Docker instances and containers, find Docker Doomsday, and fix it with a security patch using TrueSight Server Automation.

Thinking back to Benjamin Franklin, your ounce of prevention is patching with BMC TrueSight Server Automation. But do it soon, time favors the attacker, not the defender.