Written by Frederick Douglas
14 February 2019

Researchers warn of a serious vulnerability in container technology-- one possibly allowing attackers to enable malicious containers to escape the confines of the isolated process segment, gaining access to the host operating system in the process.

"The vulnerability allows a malicious container to (with minimal user interaction) overwrite the host runc binary and thus gain root-level code execution on the host," SUSE senior engineer Aleksa Sarai writes in an advisory.

Dubbed CVE-2019-5736, the vulnerability involves runc, the open source command line utility designed to spawn and run containers. It is used as the default runtime for containers with Docker, containerd, Podman and CRI-O. The running container application is supposed to be isolated from the underlying operating system, but the vulnerability allows access to the underlying operating system, putting all containers running on the host (and the host itself) at risk.

Researchers say the vulnerability is automatically blocked on systems where namespaces are used correctly, meaning containers running as root are not affected. However it impacts machines where "the host root is mapped into the container's user namespace," since the default AppArmor policy and Fedora default SELinux policy do not block CVE-2019-5736.

A patch is already available in the upstream runc project, and multiple vendors and cloud providers are pushing updates as necessary. For instance, Google admits CVE-2019-5736 affects Google Kubernetes Engine (GKE) Ubuntu nodes. It also hits multiple AWS services, including Amazon Linux, Amazon Elastic Container Service (ECS), Elastic Container Service for Kubernetes (EKS), AWS Fargate, IoT Greengrass, AWS Batch, Elastic Beanstalk, Cloud9, Sagemaker, RoboMaker and the Deep Learning AMI.

As for other container vendors, Red Hat advises customers to update as it points out the mitigating controls available through SELinux.

Go CVE-2019-5736 runc Container Breakout Advisory