CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-003

RunC Vulnerability Affecting Container Management Systems

February 13, 2019 — v1.0

TLP:WHITE

History:

- *13/02/2019 — v1.0 – Initial publication*

Summary

A container breakout security flaw was found in underlying software used by *containerization* software (operating-system-level virtualization software) [1]. The vulnerability – CVE-2019-5736 – dubbed `runc` *container breakout* allows specially crafted containers to gain administrative privileges on the host [2].

Technical Details

`runc` is an open source command line utility [3] designed to spawn and run containers, and it is used as the default runtime for containers with **Docker**, **containerd**, **Podman**, and **CRI-O**. The vulnerability allows a malicious container to overwrite the host `runc` binary – with minimal user interaction – and thus gain root-level code execution on the host [1].

The attack involves replacing the target binary in the container with one that refers back to the `runc` binary. This can be done by attaching a privileged container (connecting it to the terminal) or starting it with a malicious image and making it execute itself. The Linux kernel normally would not allow the `runc` binary on the host to be overwritten while `runc` is executing. To overcome this, the attacker can instead open a file descriptor to `/proc/self/exe` using the `O_PATH` flag and then proceed to reopen the binary as `O_WRONLY` through `/proc/self/fd/<nr>` and try to write to it in a busy loop from a separate process. It will succeed when the `runc` binary exits [4].

In some environments – for example DevOps – unintentional activation of malicious dependencies would lead to compromise of the environment. So, even if clean images are used – without patching the `runc` – infection can still happen by usage of compromised dependencies or libraries. This is why patching is paramount in this case.

The researchers announced they will publish exploit code on 18/02/2019 [1]. There are already publicly available proof-of-concepts on the Internet [5].

Products Affected

Container software like: **Docker**, **cri-o**, **containerd**, **Kubernetes** and others. Also the cloud providers are affected [6].

Recommendations

If you have a container environment verify that you are not vulnerable. For patching a list with references is provided in [2].

References

[1] https://seclists.org/oss-sec/2019/q1/119

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5736

[3] https://github.com/opencontainers/runc

[4] https://www.theregister.co.uk/2019/02/11/docker_container_flaw/

[5] https://github.com/feexd/pocs/blob/master/CVE-2019-5736/exploit.c

[6] https://aws.amazon.com/security/security-bulletins/AWS-2019-002/