Hive Pro

# THREAT ADVISORY

## Linux Distributions affected by a privilege escalation vulnerability

**TA2022048**

**Threat Level** AMBER

**Publish Date –** March 7, 2022

A new privilege escalation vulnerability has been reported that affects all the major releases of the Linux kernel and being tracked as CVE-2022-0492. The issue primarily affects the Linux kernel feature known as control groups (groups), which controls, accounts for, and isolates a collection of processes' resource utilization (CPU, memory, disk I/O, network, etc). A local attacker can exploit this issue to escape a container to execute arbitrary commands and gain admin privileges of the container host.

The flaw exists in the Linux kernel because it fails to properly restrict access to the cgroups 'release_ agent' feature that under certain circumstances allows it to escalate privileges and bypass the namespace isolation. Specifically, the vulnerability occurs due to an implementation error in the 'cgroup_release_agent_write()' function of the 'kernel/cgroup/cgroup-v1.c' file.

This vulnerability affects all major Linux distributions, and organizations make use of the script to detect whether they are impacted. Organizations can also make use of the mitigations provided by the researchers to mitigate the risk. However, this issue has been fixed in all the latest versions of Linux.

Potential MITRE ATT&CK TTPs are:
TA0004: Privilege Escalation
T1611: Escape to Host
T1068: Exploitation for Privilege Escalation
TA0003: Persistence
T1098: Account Manipulation

## Vulnerability Detail

| CVE ID | Vulnerability Name | CWE ID |
|---|---|---|
| CVE-2022-0492 | Linux Kernel privilege escalation Vulnerability | CWE-287 |

## Patch Link

https://oss.oracle.com/ol7/SRPMS-updates/kernel-uek-container-5.4.17-2136.302.7.2.3.el7.src.rpm
https://oss.oracle.com/ol7/SRPMS-updates/kernel-uek-5.4.17-2136.302.7.2.3.el7uek.src.rpm
https://oss.oracle.com/ol8/SRPMS-updates/kernel-uek-container-5.4.17-2136.302.7.2.3.el8.src.rpm
https://oss.oracle.com/ol8/SRPMS-updates/kernel-uek-5.4.17-2136.302.7.2.3.el8uek.src.rpm

## References

https://unit42.paloaltonetworks.com/cve-2022-0492-cgroups/
https://security-tracker.debian.org/tracker/CVE-2022-0492
https://ubuntu.com/security/cve-2022-0492
https://access.redhat.com/security/cve/cve-2022-0492
https://www.suse.com/security/cve/CVE-2022-0492.html
https://advisories.mageia.org/MGASA-2022-0063.html