Hive Pro

THREAT ADVISORY

Privilege Escalation Vulnerability in Snap Package Manager puts Linux users at risk

TA2022038

Threat Level AMBER

Publish Date – Feb 18, 2022

A privilege escalation vulnerability has been identified in Canonical Snap software package manager that affects the Linux-based operating systems. Successful exploitation of this issue might allow an attacker to escalate privileges and gain root access to the affected system.

The issue being tracked as CVE-2021-44731 exists due to a race condition in the 'snap-confine' function, a program used internally by snapd to construct the execution environment for snap applications. A local attacker can use this flaw to gain root privileges by bind-mounting their own contents inside the snap's private mount namespace and causing 'snap-confine' function to run arbitrary code.

To address this vulnerability, organizations should upgrade their snap (package manager) to versions 2.54.3+18.04, 2.54.3+20.04, and 2.54.3+21.10.1.

Potential MITRE ATT&CK TTPs are:
TA0004: Privilege Escalation
T1068- Exploitation for Privilege Escalation

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-44731	snapd version 2.54.2	cpe:2.3:a:canonical:snapd:2.54.2:*:*:*:*:*:*:*	Race condition in snap-confine's setup_private_mount()	CWE-362

Patch Link

https://ubuntu.com/security/notices/USN-5292-1

References

https://blog.qualys.com/vulnerabilities-threat-research/2022/02/17/oh-snap-more-lemmings-local-privilege-escalation-vulnerability-discovered-in-snap-confine-cve-2021-44731