# CVE Detail – CVE-2022-20141

In ip\_check\_mc\_rcu of igmp.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege when opening and closing inet sockets with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-112551163References: Upstream kernel

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.08051

## CVSS Scoring

CVSS v3.1 Score: 7.0

Severity: HIGH

## Mapped CWE(s)

* CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
* CWE-416: Use After Free
* CWE-667: Improper Locking

## CAPEC(s)

* CAPEC-25: Forced Deadlock
* CAPEC-26: Leveraging Race Conditions
* CAPEC-27: Leveraging Race Conditions via Symbolic Links
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions

## ATT&CK Techniques

* T1499.004: Application or System Exploitation

## Used By (Actors/Tools)

* Industroyer (malware)

## Affected Products

* cpe:2.3:o:google:android:-:\*:\*:\*:\*:\*:\*:\*