Exploitability of CVE-2021-43267

As this vulnerability was discovered within a year of its introduction into the codebase, TIPC users should ensure that they update to a patched version.

**Remediation**

This patch moves the size validation to take place in the kernel heap, as opposed to the user-space API. The kernel heap validation will be stricter than the API, which will prevent overflow.

```c
u16 key_gen = msg_key_gen(hdr);
if (unlikely(msz < hsz))
    goto exit_unlock;
if (unlikely(hsz < MIN_H_SIZE) || (hsz > MAX_H_SIZE))
    return;
```

**Executive Summary**

CVE-2021-43267: Remote Linux Kernel Heap Overflow

**Description**

Transparent Inter-Process Communication (TIPC) is a protocol that allows nodes in a cluster to communicate with each other in a way that can optimally handle a large number of nodes remaining fault tolerant.

**Vulnerability**

The vulnerability can be exploited either locally or remotely within a network to gain kernel privileges, allowing an attacker to escalate their privileges.

**Impact**

The impact of this vulnerability is significant, as it allows attackers to escalate privileges within the system.

**Remediation**

A patch has been released on the 29th of October and affects kernel versions between 5.10 and 5.15. This patch moves the size validation to take place in the kernel heap, as opposed to the user-space API. The kernel heap validation will be stricter than the API, which will prevent overflow.

**CodeQL Analysis**

For those who haven't come across it before, CodeQL is an analysis engine that allows you to run queries on code. From there, you can use it to identify potential vulnerabilities in code. SentinelLabs started using CodeQL for their own research on open source projects and decided to compile the Linux kernel with it and analyze it for vulnerabilities.

**SentinelLabs Response**

SentinelLabs supplied the initial vulnerability report to the Kernel.org team on the 19th of October. Greg K.H. responded and added the TIPC maintainers to the email thread on the same day.

**Patch**

The patch was added to lore.kernel.org on the 25th of October.

**SentinelOne Response**

At this time, SentinelOne has not identified evidence of in-the-wild abuse.

**SentinelOne Roadmap**

For the remainder of 2021, SentinelOne plans to focus on improving their analysis techniques and expanding their coverage of open source projects.

**Contact**

If you have any questions or concerns regarding this vulnerability, please contact SentinelOne at info@sentinelone.com.