



CVE-2022-20154

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2022-20154 |
| State | PUBLIC |
| Assigner | security@android.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-06-15 14:15:00 UTC |
| Updated | 2022-06-24 02:05:00 UTC |
| Description | In lock_sock_nested of sock.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with local privileges. |

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | Google | Android | - | All | All | All |

References

| Reference | Source | Link | Tags |
|---------------------------------------------------------------|---------|-------------------------------------------------------------|---------------------|
| Pixel Update Bulletin—June 2022 Android Open Source Project | MISC | source.android.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|----------------------------------------------------------------------------------------------------|
| 179361 Debian Security Update for linux (CVE-2022-20154) |
| 376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125) |
| 610418 Google Pixel Android June 2022 Security Patch Missing |
| 672086 EulerOS Security Update for kernel (EulerOS-SA-2022-2321) |
| 672114 EulerOS Security Update for kernel (EulerOS-SA-2022-2292) |

| |
|------------------------------------------------------------------------------------------------------------------------|
| 672139 EulerOS Security Update for kernel (EulerOS-SA-2022-2428) |
| 672158 EulerOS Security Update for kernel (EulerOS-SA-2022-2415) |
| 672205 EulerOS Security Update for kernel (EulerOS-SA-2022-2466) |
| 752340 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2377-1) |
| 752349 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2382-1) |
| 752354 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2393-1) |
| 752359 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2411-1) |
| 752360 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2407-1) |
| 752363 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2423-1) |
| 752364 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2422-1) |
| 752370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1) |
| 752391 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2549-1) |
| 752463 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2809-1) |
| 753148 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1) |
| 753214 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 19 for SLE 15 SP3) (SUSE-SU-2022:2515-1) |
| 753271 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2424-1) |
| 753282 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 31 for SLE 15 SP1) (SUSE-SU-2022:2435-1) |
| 753323 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15) (SUSE-SU-2022:2460-1) |
| 753362 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2376-1) |
| 753363 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP1) (SUSE-SU-2022:2461-1) |
| 753415 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 20 for SLE 15 SP3) (SUSE-SU-2022:2516-1) |
| 753420 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15) (SUSE-SU-2022:2482-1) |
| 755966 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2024:0857-1) |
| 755988 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0975-1) |
| 756004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0926-1) |
| 756005 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0925-1) |

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)