

CVE-2024-36971

Android Kernel Remote Code Execution Vulnerability

CISA KEV since Aug 7, 2024

Actively exploited

In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advice() uses the wrong order.

EVRS

75/100

Urgent priority

CVSS V3.1

7.8

High · NVD

EPSS

0.027

85.8th percentile · FIRST

CISA DEADLINE

Aug 28, 2024

KEV since 2024 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.027 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA****note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.

Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Given that ip6_negative_advice() has special logic against RTE_CACHE, this means each of the three ->negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advice(), there is no need to duplicate it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
debian linux	10.0	no fixed version listed	NVD
linux kernel	≥ 4.6 < 4.19.316 ≥ 4.20 < 5.4.278 ≥ 5.5 < 5.10.219 ≥ 5.11 < 5.15.161 ≥ 5.16 < 6.1.94 ≥ 6.2 < 6.6.34 ≥ 6.7 < 6.9.4	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/stable/c/051c0bde9f0450a2ec3d62a86d2a0d2fad117f13	source.android.com/docs/security/bulletin/2024-08-01 , https://lore.kernel.org/linux-cve-announce/20240610090330.1347021-2-lee@kernel.org/T/#u	source.android.com/docs/security/bulletin/2024-08-01 , https://lore.kernel.org/linux-cve-announce/20240610090330.1347021-2-lee@kernel.org/T/#u
NVD	nvd.nist.gov/vuln/detail/CVE-2024-36971	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-36321	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-36971

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.