



Race condition vulnerability in Linux kernel bluetooth sniff_{min,max}_interval_set()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-24859
State	PUBLISHED
Assigner	Anolis
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-05 08:15:44 UTC
Updated	2026-05-12 12:16:18 UTC
Description	A race condition was found in the Linux kernel's net/bluetooth in sniff_{min,max}_interval_set() function. This can result in a

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H

EPSS: 0.000080000 probability, percentile 0.007900000 (date 2026-05-12)

Problem Types: CWE-362 | CWE-362 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	security@openanolis.org	Secondary	4.6	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:H
3.1	CNA	CVSS	4.6	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	6.8	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Linux	Linux Kernel	affected v4.0-rc1 v6.8-rc2 custom	Linux, x86, ARM
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom	Not specified

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
Bug Access Denied	af854a3a-2127-422b-91ae-364da2661108	bugzilla.openanolis.cn	Issue Tracked
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: 白家驹 <baijiaju@buaa.edu.cn> (en)

CNA: 韩桂栋 <hanguidong@buaa.edu.cn> (en)

Additional Advisory Data

Solutions

CNA: <https://lore.kernel.org/lkml/20231222162931.6553-1-2045gemini@gmail.com/>
<https://lore.kernel.org/lkml/20231222162931.6553-1-2045gemini@gmail.com/>

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

Free CVE JSON API [cve.report/api](#)

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