rseq: Fix segfault on registration when rseq_cs is non-zero

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-38067
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-18 10:15:39 UTC
Updated	2026-05-12 13:16:42 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: rseq: Fix segfault on registration when rseq_cs is non-zero

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability
High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 48900d839a345
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 3e4028ef31b69
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 b2b05d0dc2f4f0
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 eaf112069a904
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 f004f58d18a2d3
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 2df285dab00fa0
CNA	Linux	Linux	affected d7822b1e24f2df5df98c76f0e94a5416349ff759 fd881d0a085fc5
CNA	Linux	Linux	affected 4.18
CNA	Linux	Linux	unaffected 4.18 semver
CNA	Linux	Linux	unaffected 5.10.240 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.189 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.146 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.99 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.39 6.12.* semver
CNA	Linux	Linux	unaffected 6.14.9 6.14.* semver
CNA	Linux	Linux	unaffected 6.15 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link
git.kernel.org/stable/c/2df285dab00fa03a3ef939b6cb0d0d0aeb0791db	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/b2b05d0dc2f4f0646922068af435aed5763d16ba	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/48900d839a3454050fd5822e34be8d54c4ec9b86	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/fd881d0a085fc54354414aed990ccf05f282ba53	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/3e4028ef31b69286c9d4878cee0330235f53f218	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/eaf112069a904b6207b4106ff083e0208232a2eb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f004f58d18a2d3dc761cf973ad27b4a5997bd876	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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