Triaging CVEs for the Linux Kernel

Automating the assessment of Kernel Vulnerabilities

SIEMENS

Civil Infrastructure Platform (CIP)

- Part of the Linux Foundation
- Linux Kernels for Industrial Applications
- Provides Super-Long-Term Support kernels (~10 years after mainline support ends)

CIVIL INFRASTRUCTURE PLATFORM

INDUSTRIAL GRADE LINUX

Version	Maintainer(s)	First Release	Projected EOL	Target Releases/Month*
SLTS v6.12	Nobuhiro Iwamatsu & Pavel Machek	2025-05-20	2035-06	2
SLTS v6.1	Nobuhiro Iwamatsu & Pavel Machek	2023-07-14	2033-08	1
SLTS v6.1-rt	Pavel Machek	2023-07-16	2033-08	0.5
SLTS v5.10	Nobuhiro Iwamatsu & Pavel Machek	2021-12-05	2031-01	1
SLTS v5.10-rt	Pavel Machek	2021-12-08	2031-01	0.5
SLTS v4.19	Ulrich Hecht	2019-01-11	2029-01	1
SLTS v4.19-rt	Pavel Machek	2019-01-11	2029-01	0.5
SLTS v4.4	Ulrich Hecht	2017-01-17	2027-01	1
SLTS v4.4-rt	Pavel Machek	2017-11-16	2027-01	0.5

SIEMENS

Why do we need to do anything?

- CRA is looming on the horizon
- Older kernel versions accrue hundreds to thousands of unfixed CVEs (EOL of 4.19 had ~1000 CVEs)
- Updating to newer kernels is not always possible

CVEs in the Kernel

- Kernel Team started issuing CVEs as a CNA in February 2024
- Around 60 CVEs each week
- CVEs are always published **after** a fix is available

```
From: Greg Kroah-Hartman <gregkh@kernel.org>

Description
===========

In the Linux kernel, the following vulnerability has been resolved:

KVM: arm64: Fix uninitialized memcache pointer in user_mem_abort()

Commit fce886a60207 ("KVM: arm64: Plumb the pKVM MMU in KVM") made the
initialization of the local memcache variable in user_mem_abort()
conditional, leaving a codepath where it is used uninitialized via
kvm_pgtable_stage2_map().

This can fail on any path that requires a stage-2 allocation
without transition via a permission fault or dirty logging.

Fix this by making sure that memcache is always valid.

The Linux kernel CVE team has assigned CVE-2025-37996 to this issue.


Affected and fixed versions
===========================

        Issue introduced in 6.14 with commit fce886a6020734d6253c2c5a3bc285e385cc5496 and fixed in 6.14.7 with commit a26d50f8a4a5049e956984797b5d0dedea4bbb18
        Issue introduced in 6.14 with commit fce886a6020734d6253c2c5a3bc285e385cc5496 and fixed in 6.15 with commit 157dbc4a321f5bb6f8b6c724d12ba720a90f1a7c

Please see https://www.kernel.org for a full list of currently supported
kernel versions by the kernel community.

Unaffected versions might change over time as fixes are backported to
older supported kernel versions.  The official CVE entry at
        https://cve.org/CVERecord/?id=CVE-2025-37996
will be updated if fixes are backported, please check that for the most
up to date information about this issue.


Affected files
==============

The file(s) affected by this issue are:
        arch/arm64/kvm/mmu.c
```

Know your Use-case

- Linux has ~85.000 files, ~40.000.000 LoC
- Typically only about 5% to 10% are used
- Almost all of the CVEs will not be relevant for your specific use-case
- **Checking this is on you, nobody will do it for you**

Goals

- Given a kernel version, a use-case and a CVE:
  assess if the CVE is relevant
- Be fast
- No false negatives
- Provide useful information for vulnerability remediation
  in a standard format

Implementation

- Use-case is described by a Kconfig
- Run a number of checks for each CVE, each giving a "relevant"/"not relevant" verdict
- Each check is conservative in its assessment
- Short circuit on a "not relevant" verdict
- Simple checks based on introducing/fixing commits
- More sophisticated checks assess if files affected by the CVE are used

Results


```
"check_results": [
    {
        "name": "check_ignore",
        "result": "relevant",
        "reason": "no ignore"
    },
    {
        "name": "check_introduced_by",
        "result": "relevant",
        "reason": "found 2014fcea19ec27df033359a0f42db0e8ed4290a8"
    },
    {
        "name": "check_introduced_by_file_compiled",
        "objects": [
            {
                "name": "drivers/mtd/nand/raw/atmel/pmecc.o",
                "built": false,
                "config": "CONFIG_MTD_NAND_ATMEL && CONFIG_MTD"
            },
            {
                "name": "drivers/mtd/nand/raw/atmel/nand-controller.o",
                "built": false,
                "config": "CONFIG_MTD_NAND_ATMEL && CONFIG_MTD"
            }
        ],
        "deleted_files": [],
        "result": "not relevant",
        "reason": "no file is compiled"
    }
]
```

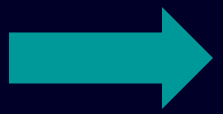

In vex format:


```
{
"vulnerability": {
    "name": "CVE-2024-56766",
    "description": "mtd: rawnand: fix double free in atmel_pmecc_create_user()"
},
"status": "not_affected",
"justification": "vulnerable_code_not_present"
```


SIEMENS

Results

- For CIP kernels /w CIP defconfig 90% - 95% of CVEs reported in 2024 were deemed "not relevant"
- 4.19 EOL for the unfixed ~1000 CVEs 56% can be excluded



For better results a better description of the use-case is required

Contact us!

Christoph Steiger <christoph.steiger@siemens.com>

CIP Project: https://gitlab.com/cip-project

Kernel-CVE-Triage: https://gitlab.com/cip-project/cip-kernel/kernel-cve-triage

SIEMENS