ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

TU Graz

SLUBStick

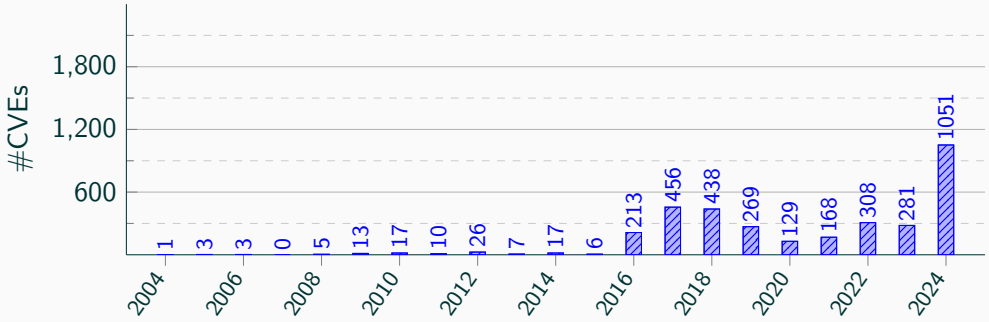
Arbitrary Memory Writes through Practical Software Cross-Cache Attacks within the Linux Kernel

Lukas Maar, Stefan Gast, Martin Unterguggenberger, Mathias Oberhuber, and Stefan Mangard

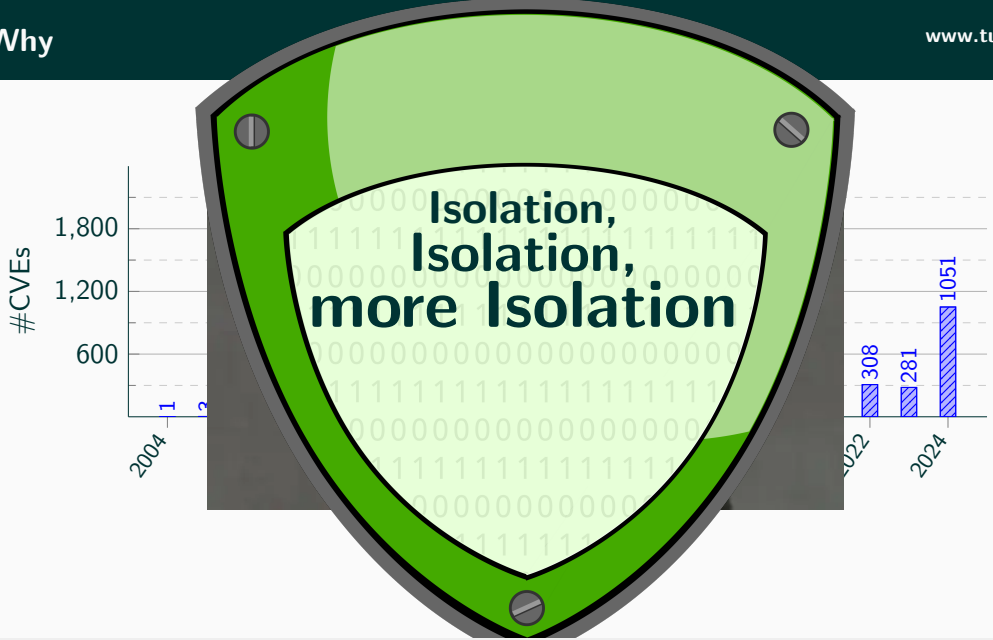
November 8, 2024

Graz University of Technology

The Why


#CVEs
1,800
1,200
600
1
3
3
0
5
13
17
10
26
7
17
6
213
456
438
269
129
168
308
281
1051
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024

The Why


#CVEs
1,800
1,200
600
1
308
281
1051
2004
2024
Isolation,
Isolation,
more Isolation


#CVEs
1,800
1,200
600
2004
2024
308
281

Kernel exploit technique **SLUBStick**

Kernel exploit technique **SLUBStick**

- Timing side channel on the allocator:
  - To bypass isolation-based defenses

Kernel exploit technique **SLUBStick**

- Timing side channel on the allocator:
  - To bypass isolation-based defenses
- Primitive convertion:
  - Limited heap write to a more powerful write

Kernel exploit technique **SLUBStick**

- Timing side channel on the allocator:
  - To bypass isolation-based defenses
- Primitive convertion:
  - Limited heap write to a more powerful write
- Page-table manipulation:
  - Allows to read from and write to the entire physical memory

Kernel exploit technique **SLUBStick**

- Timing side channel on the allocator:
  - To bypass isolation-based defenses
- Primitive convertion:
  - Limited heap write to a more powerful write
- Page-table manipulation:
  - Allows to read from and write to the entire physical memory
- Implement 9 PoC exploits
  - To compromise the entire system

Real-World Exploitation


PWNED!

Real-World Exploitation


PWNED!


PWNED!


ESCAPED!
docker


PWNED!


ESCAPED!
containerd

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

TU Graz

SLUBStick

Arbitrary Memory Writes through Practical Software Cross-Cache Attacks within the Linux Kernel

Lukas Maar, Stefan Gast, Martin Unterguggenberger, Mathias Oberhuber, and Stefan Mangard

November 8, 2024

Graz University of Technology