New issue

Signed 64-bit integer overflow in RTT calculation #584

Open

Zephkek opened yesterday · edited by Zephkek Edits

Hello,

A specially crafted ICMP Echo Reply can trigger a possible signed 64-bit integer overflow in the `iputils` ping RTT calculation. This occurs due to uncontrolled multiplication of the timestamp seconds by 1,000,000, causing undefined behavior. The vulnerability may present itself as runtime errors detected by AddressSanitizer or as silent failures, resulting in repeated zero RTT readings and incorrect statistics.

Affected Versions

- `iputils ping` (current `master` branch)
- Ubuntu package version `iputils-ping 3:20240117-1build1`

Environment

- Ubuntu 24.04.1 LTS (Noble Numbat)
- Kernel: `5.15.167.4-microsoft-standard-WSL2`
- Architecture: `x86_64`

Detailed Steps and PoC

Full details, reproduction steps, and PoC script can be found here:

https://github.com/Zephkek/ping-rtt-overflow/

Bug found by Mohamed Maatallah

Zephkek changed the title ~~Signed 64-bit integer overflow in RTT calculation (`triptime = tv->tv_sec * 1000000 + tv->tv_usec`)~~ Signed 64-bit integer overflow in RTT calculation yesterday

pevik self-assigned this 6 hours ago

pevik added bug security reproducer 6 hours ago

Zephkek 1 hour ago Author •••

Hi,

The PoC is public purely to support reproducibility. If you'd prefer I make it private, just let me know.

carnil 1 hour ago · edited by carnil Edits •••

Looks this issue got CVE-2025-47268 assigned.

nmeyerhans 27 minutes ago Contributor •••

The real world security implications of this seem dubious, at best. I might get unreliable results from pinging a malicious host?

Assignees

pevik

Labels

bug reproducer security

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants