

PB173 – Ovladače jádra – Linux XIII.

Jiří Slabý

ITI, Fakulta Informatiky

20. 12. 2011

- Firmware
- Analýza OOPS

Část I

Firmware

- Binární kód v zařízení
- Nahrává jej (většinou) ovladač

API

- `linux/firmware.h`, struct firmware
- `request_firmware(const struct firmware **fw, const char *name, struct device *device)`
 - fw – návratová hodnota
 - name – jméno souboru
- `release_firmware`

```
struct firmware {
    size_t size;
    const u8 *data;
    ...
};
```

Nahrání firmware

- 1 Zkopírujte pb173/13/fw/firmware_*.bin do /lib/firmware
- 2 Nahrajte firmware v ovladači
 - V závislosti na architektuře (např. makro CONFIG_64BIT)
- 3 Zkopírujte data do spustitelné paměti
 - `_vmalloc + PAGE_KERNEL_EXEC`
- 4 V cyklu pro 0 ... 100
 - Zavolejte 0. offset alokované paměti
 - Prototyp: `unsigned int (*)(unsigned int)`
 - Vypište návratovou hodnotu
- 5 Zjistěte, co firmware dělá

Firmware v ASM

```
$ objdump -D -b binary -m i386 -M x86-64 firmware_64.bin
```

```
0: 31 c0          xor    %eax,%eax      ; eax — retval
2: 83 ff 0d      cmp    $0xd,%edi     ; edi — param 0
5: 77 14        ja     0x1b
7: 83 ff 01      cmp    $0x1,%edi
a: b0 01        mov    $0x1,%al
c: 76 0d        jbe   0x1b
e: 66 90        xchg  %ax,%ax        ; nop
10: 0f af c7     imul  %edi,%eax
13: 83 ef 01      sub    $0x1,%edi
16: 83 ff 01      cmp    $0x1,%edi
19: 75 f5        jne   0x10
1b: f3 c3        repz  retq           ; "return eax"
```

Část II

Analýza OOPS

Analýza pádů

- 1 Modul v pb173/13/oops