CVE-2020-28921

Description

The `PCADRVX64.sys` kernel driver distributed with the PC Analyser application by Devid Espenschied Software expose an IOCTL functionality that allows low-privilege users to read and write arbitrary Model Specific Registers (MSRs). This could lead to arbitrary Ring-0 code execution and escalation of privileges.

Impact

High - Arbitrary Ring-0 code execution

Exploitability

Medium/Low - Driver must be loaded prior to the exploitation in order to be utilized by low-privilege users, otherwise the attacker will require admin rights for the driver installation.

Technical Details

The driver offers a `rdmsr` and `wrmsr` functionality exposed via IOCTL that allows an unprivileged usermode program to read and write arbitrary CPU MSR. This can be leveraged by the attackers to patch the critical MSRs like `IA32_LSTAR` (`0xC0000082`) or `IA32_SYSENTER_EIP` (`0x00000176`) in order to achieve kernel code execution. Although many kernel exploit mitigation techniques exist, this is a viable exploit even on the newest Windows 10 systems with mitigations like SMEP, SMAP in place (as of November 2020). The vulnerable IOCTLs:

```
IOCTL_READ_MSR  = 0x82002000
IOCTL_WRITE_MSR = 0x82002100
```

Resolution

The fix is distributed as a part of the 4.10 update of the PC Analyser application.

Reporter

This vulnerability was discovered and reported by Michal Poslušný.

Disclosure Timeline

- 16 November 2020 - Issue reported to vendor
- 16 November 2020 - Vendor responded and confirmed the issues
- 19 November 2020 - Vendor shared a test version of the driver with the issues addressed
- 25 November 2020 - Vendor released a patch for the application with updated version of the driver

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28921
- http://www.pcanalyser.de/index.php/historie/