CVE-2020-28922

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 physical memory. 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 physical memory read and write functionality exposed via IOCTL that allows an unprivileged usermode program to read and write arbitrary physical memory. This can be utilized by the attackers to scan the memory for critical structures and code in kernel and patch them in order to directly manipulate kernel objects or achieve kernel code execution. The vulnerable IOCTLs:

```
IOCTL_READ_PHYSICAL_MEMORY_BYTE   = 0x82002400
IOCTL_READ_PHYSICAL_MEMORY_WORD   = 0x82002500
IOCTL_READ_PHYSICAL_MEMORY_DWORD  = 0x82002600

IOCTL_WRITE_PHYSICAL_MEMORY_BYTE  = 0x82002700
IOCTL_WRITE_PHYSICAL_MEMORY_WORD  = 0x82002800
IOCTL_WRITE_PHYSICAL_MEMORY_DWORD = 0x82002900
```

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-2020-28922
- http://www.pcanalyser.de/index.php/historie/