CVE-2020-15480

Description

The `DirectIo32.sys` and `DirectIo64.sys` kernel drivers distributed with the BurnInTest, PerformanceTest and OSForensics applications by PassMark 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 (as of August 2020). The vulnerable IOCTLs:

```
IOCTL_READ_MSR  = 0x80112060
IOCTL_WRITE_MSR = 0x80112088
```

Resolution

The fix is distributed as a part of the August 2020 updates of the vendor's products.

Reporter

This vulnerability was discovered and reported by Michal Poslušný.

Disclosure Timeline

- 23 June 2020 - Issue reported to vendor
- 23 June 2020 - Vendor responded and confirmed the issues
- 15 July 2020 - Vendor shared a test version of the driver with the issues addressed
- 24 July 2020 - Vendor released a final version of the driver
- 6 August 2020 - Integration of the fixed version of the driver into the vendor's products started

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15480
- https://www.passmark.com/products/performancetest/history.php