eset / vulnerability-disclosures Public

Code Issues Pull requests Projects Security Insights

master

vulnerability-disclosures / CVE-2020-15481 / CVE-2020-15481.md

mposlusny Add details about CVE-2020-15481 History

1 contributor

54 lines (37 sloc) | 1.81 KB

CVE-2020-15481

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 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 mapping 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_MAP_PHYSICAL_MEMORY = 0x80112044
```

Resolution

The fix is distributed as a part of the September 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
- 9 September 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-2020-15481
- https://www.passmark.com/products/performancetest/history.php