eset / vulnerability-disclosures Public

Code Issues Pull requests Projects Security Insights

master

vulnerability-disclosures / CVE-2020-15479 / CVE-2020-15479.md

mposlusny Add details about CVE-2020-15479 and CVE-2020-15480 History

1 contributor

53 lines (37 sloc) | 1.86 KB

CVE-2020-15479

Description

The IOCTL request handler in the `DirectIo32.sys` and `DirectIo64.sys` kernel drivers distributed with the BurnInTest, PerformanceTest and OSForensics applications by PassMark Software attempts to copy the input buffer onto the stack without checking its size and can cause a buffer overflow. 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

When the driver receives an IOCTL request from a usermode program, it will first copy the request input buffer into a local buffer on the stack. The size of the memcpy is only based on the size of the input buffer and does not take into account the capacity of the stack buffer. This may lead to a buffer overflow, if a large enough IOCTL buffer is provided. This happens in multiple places of the IOCTL handler function and several IOCTLs can be used for this purpose.

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-2020-15479
- https://www.passmark.com/products/performancetest/history.php