Rootshell Discover a Denial of Service Flaw in Dekart Private Disk Encryption Software

The Rootshell Security team have discovered a flaw in Dekart Private Disk; a hard disk encryption software for Windows sold by Dekart, an IT security software company.

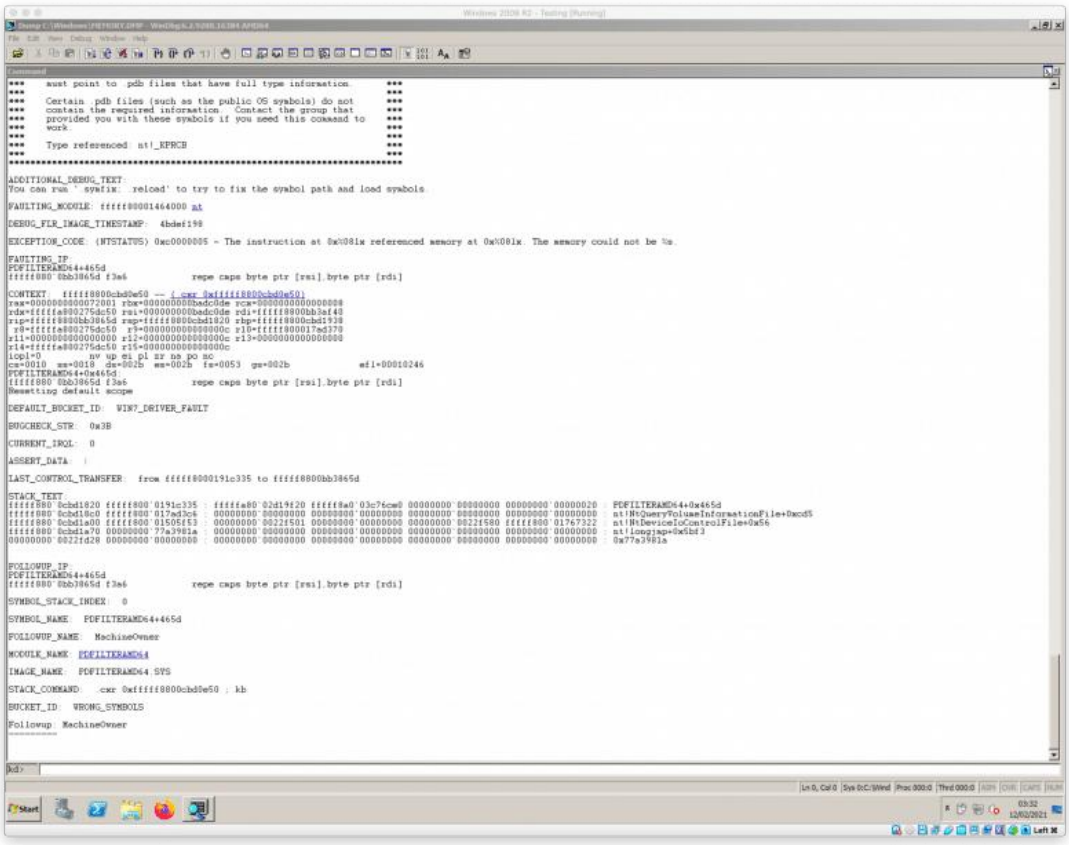
The flaw, which seems to affect every version of Dekart Private Disk, occurs when a local user or program sends an input/output control (IOCTL) request to the kernel driver. This can cause the driver to dereference arbitrary memory, which has the potential to crash the system with a BSOD (the dreaded 'Blue Screen of Death').

The root cause of the issue is in validating the buffer sent from the user to the kernel driver. The software seeks to validate that the request has come from the userland components of the implementation (i.e. the code that runs outside of the kernel), by comparing the first 4 bytes of the request against a constant (magic) value.

However, this check is performed prior to accessing and validating the code from the IOCTL request, meaning the 8 byte flag is read from the Type3 pointer. Therefore, should the IOCTL code be METHOD_NEITHER, the pointer could reference invalid or un-paged memory and cause the driver to page-fault. This is shown below.

```
.text:000000000001463F    loc_1463F:                    ; CODE XREF: sub_145A0+8A↑j
.text:000000000001463F                                  ; sub_145A0+8F↑j ...
.text:000000000001463F 098          test    rbx, rbx
.text:0000000000014642 098          jz      short loc_14672
.text:0000000000014644 098          cmp     r15d, 0Ch
.text:0000000000014648 098          jb      loc_14CDE
.text:000000000001464E 098          lea     rdi, aPrvdmon   ; "PRVDMON"
.text:0000000000014655 098          mov     rsi, rbx
.text:0000000000014658 098          mov     ecx, 8
.text:000000000001465D 098          repe cmpsb
.text:000000000001465F 098          jnz     loc_14CDE
.text:0000000000014665 098          mov     rbx, [rsp+98h+arg_20]
.text:000000000001466D 098          test    rbx, rbx
.text:0000000000014670 098          jnz     short loc_14680
```

The Rootshell team have created a simple proof-of-concept (PoC) to demonstrate the issue, which will crash any affected system.



In line with our Bug Release Terms, we informed Dekart of the vulnerability and gave 90 days of notice before disclosing it. Further disclosures in the same products are yet to be submitted, but since the issue is limited to a Denial of Service (DoS), the severity of the release is limited and doesn't pose security risks to the user.

Led by Rootshell's Head of Research and Development, Dr Neil Kettle, our research ensures we continue to play an important role in encouraging vendors to implement best practice software development for the benefit and protection of users.

The bug has been catalogued as CVE-2021-27203.

Read our previous bug releases:

Rootshell Discover KeyScrambler Security Flaw That Enables Encryption To Be Bypassed

Rootshell Discover Remote Heap Corruption Bug Within MiniDLNA And Develop Proof Of Concept Exploit

Related Posts

info@rootshellsecurity.net

UK +44 1256 596523

USA +1 332 225 1894

Red Team as a Service

Managed Vulnerability Scanning

Vulnerability Management System

Vulnerability Management Dashboard

Vulnerability Management Prioritization

Vulnerability Management Reports

Vulnerability Remediation Tracker

Careers