联想技术支持与 BIOS / UEFI 固件团队 · 2026 年 11 月 9 日

ThinkBook 16 G5+ APO 反复黑屏死机

机型 21J2 | BIOS MFCN38WW | Windows 11 家庭中文版 26H2（26300.9711）

一 问题总结

我的电脑多次突然黑屏、无响应，部分故障需长按电源键才能重新启动。曾在插拔 3.5 毫米耳机或启动 Steam 游戏时遇到，也出现过未操作、未连接耳机的情况。Windows 记录的停止代码为 **0xD1**。

三次有内核转储的故障均发生在 Windows 读取 UEFI 固件变量时，最终停在同一条 BIOS 指令上。请转交 BIOS / UEFI 固件团队，核查变量缓存起始地址为何会为零，并提供适用于 21J2 的处理方案。

二 问题分析与证据

三次内核转储记录。下表时间均取自转储，使用北京时间。

故障时间（2026 年）	当时情况（用户回忆）	转储中的读取方和固件变量
10 月 30 日 00:50:40.408	拔掉有线耳机后黑屏，长按电源重启。	承载 ClipSVC 的 svchost.exe 读取 OfflineUniqueIDEKPub
11 月 2 日 17:52:54.453	当时没有主动操作。	承载 ClipSVC 的 svchost.exe 读取 OfflineUniqueIDEKPub
11 月 9 日 17:54:45.751	未操作、未连接耳机，长按电源重启。	SrTasks.exe 读取启动顺序变量 BootOrder

直接故障位置。 三份转储均进入 UEFI 的 GetVariable 读取服务，在 VariableRuntimeDxe+0x1170 执行 CLFLUSH [RCX] 时，寄存器 RCX 为 0。三次故障指令所在的整页代码（4,096 字节）彼此相同，也与联想签名 MFCN38WW 镜像中的对应页面逐字节一致。

已试措施和触发条件。 10 月 30 日的音频端点事件距故障约 0.48 秒。之后关闭有线耳机音频增强，11 月 2 日仍复现。11 月 3 日禁用 ClipSVC 后，11 月 9 日再次复现。该次转储确认服务启动配置为禁用，故障线程属于 SrTasks.exe。这表明在没有插拔耳机、由另一个进程读取不同变量时，也能复现同一故障。

11 月 9 日现场参数。 0xD1 (0x0, 0xFF, 0x0, 0xFFFFF804357A9170)。转储中的 Windows 跟踪记录显示，系统当时在后台安装应用更新。“画图”开始安装与故障相隔约 0.54 秒。该时间关系没有提供固件指针曾被应用改写的证据。

二 问题分析与证据（续）

空地址从何而来。 对照转储中的寄存器、栈和官方固件指令，可反推出缓存刷新函数收到起点 0、长度非零。反汇编显示，MFCN38WW 从固件上下文 P 的八字节字段 P+0x98 取起点，随后在 +0x4965 调刷新函数。这条路径会跳过零长度，但在刷新前没有检查起点是否为空。

一个可验证的上游原因。 在 ReadyToBoot 阶段，固件调用 +0xC028 检查变量存储剩余空间和 NeedDoReclaim 标志。如果需要维护且底层操作返回错误，可经 +0xBAC5 进入 +0xCC1C，其中一条分支在 +0xCC4F 将同一字段清零。现有转储没有收录该字段所在的固件页。对 11 月 9 日的 48 个附加数据块及前两次对照样本解码，也未恢复该字段的写入历史或前序 EFI 返回码。尚不能确定故障前走过这条分支。

其他机型的官方补丁。 ARP 的 LECN19WW → LECN20WW 和 ARH 的 KJCN31WW → KJCN32WW 都列出 Insyde 补丁 IB02961583，用于解决 S4 休眠或冷启动压力测试中的 0xD1（问题 IB18390195）。两组新版二进制均把上述维护检查从 ReadyToBoot 移至固件管理模式锁定前的检查点。ARP 两版的 GetVariable 都保留了原有的缓存刷新路径。

本机型的版本对照。 联想 APO 页面公开的 10 版 BIOS 均保留原调用时机。25 / 26 / 27、29 / 30 / 32 / 33、35 / 36 / 38 分别具有组内完全相同的 VariableRuntimeDxe 模块。截至 2026 年 11 月 9 日，官网最新为本机所用的 MFCN38WW。两款对照机型同批还合入多项修复，公开资料不能把这一代码改动唯一对应到 IB02961583。

联想官方版本记录 本机 APO · 对照机型 ARP · 对照机型 ARH

三 请联想核实的内容

1. 核对已知问题及修复范围。 请查 IB18390195 的原始故障栈及 IB02961583 的变更清单，确认是否涉及上述变量维护时机或 GetVariable 对地址 0 执行 CLFLUSH。请说明 APO 的 MFCN 分支是否已有等效修复、对应的版本号和验证结果。

2. 定位缓存地址首次异常的环节。 请在同一次启动中记录 P+0x98 的初始化、每次改写的旧值和新值、写入位置、DXE / SMM 上下文，以及维护操作和 ConvertPointer 的 EFI 返回码。请核实起点为零时，为何非零长度仍能通过检查并进入刷新路径。

3. 提供可执行的处理方案。 请提供适用于 21J2 的正式修复版本，或经验证的临时规避方案。如需继续采集，请提供适配的诊断 BIOS 或签名工具，在现有硬件上安全保存目标固件页和上述写入历史，并说明原始 DMP 的官方提交渠道。