精选快讯　软件快讯　2026年11月18日 14:05

Claude Code代理因变量展开错误误删文件，开发者发布钩子拦截危险命令

要点

- Claude Code issue tracker 近期出现多起代理执行破坏性命令导致文件丢失的事故报告。
- 技术分析指出，当变量为空时，rm -rf "$D"/ 等同于 rm -rf /，而 set -u 仅在看到未设置变量的 shell 中生效，无法防止跨 shell 层的变量展开错误。
- claude-bulkhead 的 rm-empty-var 规则会拦截路径为变量或命令替换后接斜杠的递归删除命令，以及 rsync --delete 目标为 $R/ 或裸 $R 的命令。

Claude Code issue tracker 近期出现多起代理执行破坏性命令导致文件丢失的事故报告。在事故 #95426 中，代理在 Windows Git Bash 环境下执行 rm -rf "$(cygpath -u 'C:\')" 命令，导致约 600GB 数据丢失，涉及 Windows 用户资料及多个 git 仓库。事故 #109735 显示，代理通过 WSL 执行 rsync 命令时，因变量 R 在外层 shell 未定义，目标路径解析为根目录 /，进而删除了 Windows 数据盘挂载点 /mnt/d 下的文件。此外，事故 #107274 中，macOS 环境下的代理执行 rm -rf .git 命令，直接删除了仓库的 .git 目录，造成未推送的历史记录永久丢失。

技术分析指出，当变量为空时，rm -rf "$D"/ 等同于 rm -rf /，而 set -u 仅在看到未设置变量的 shell 中生效，无法防止跨 shell 层的变量展开错误。使用 ${D:?} 语法可在变量为空或未设置时使 shell 停止执行，从而防止命令替换为空字符串。针对上述风险，开发者发布了 claude-bulkhead 钩子集合，其 0.4.0 版本新增了对三种危险命令模式的拦截规则，旨在从执行层面阻断此类误操作。

claude-bulkhead 的 rm-empty-var 规则会拦截路径为变量或命令替换后接斜杠的递归删除命令，以及 rsync --delete 目标为 $R/ 或裸 $R 的命令。rm-git-dir 规则专门拦截 rm -rf .git 等命令，并建议改用 git worktree remove 或移动目录。rm-unquoted-var 规则则拦截未加引号的 rm -rf $D，防止当同一行设置的值包含空格或通配符时，bash 将其拆分为多个路径导致意外删除。

报道来源：hackernoon

来源网站：https://www.inews.today/