

微软升级64位Vista拦截未签名驱动加载 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/259/2021_2022__E5_BE_AE_E8_BD_AF_E5_8D_87_E7_c100_259000.htm 微软对其64位版本的Vista操作系统进行了升级以防止操作系统内核加载未签名代码。上周软件资讯栏目报道过，Linchpin实验室推出的Atsiv工具能够在Vista上加载未获得签名的遗留驱动程序，微软此举防止了类似事件的发生，它表示这个Atsiv工具与其内核模式代码签名(KMCS)策略相冲突。微软安全架构师Scott Field表示，在64位的Vista中，默认的KMCS策略只运行那些带有有效代码签名证书并获得数字签名的代码加载到内核之中。通过在64位Vista上进行强制内核级驱动签名，微软希望能够阻止带有rootkit行为特性的恶意驱动程序的出现。此外，微软的Windows Defender特征库也升级到8月2号，现在它也可以检测、拦截并清除最新版本的Atsiv驱动。目前Linchpin实验室并没有对此事作出评论，但预计它会相应的作出升级。100Test下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com