“盗版Win11要被封杀？”微软发布TPM新规引发恐慌，真相来了：其实没打算追究个人用户

CSDN 2026年7月28日 16:30 江苏

整理 | 郑丽媛

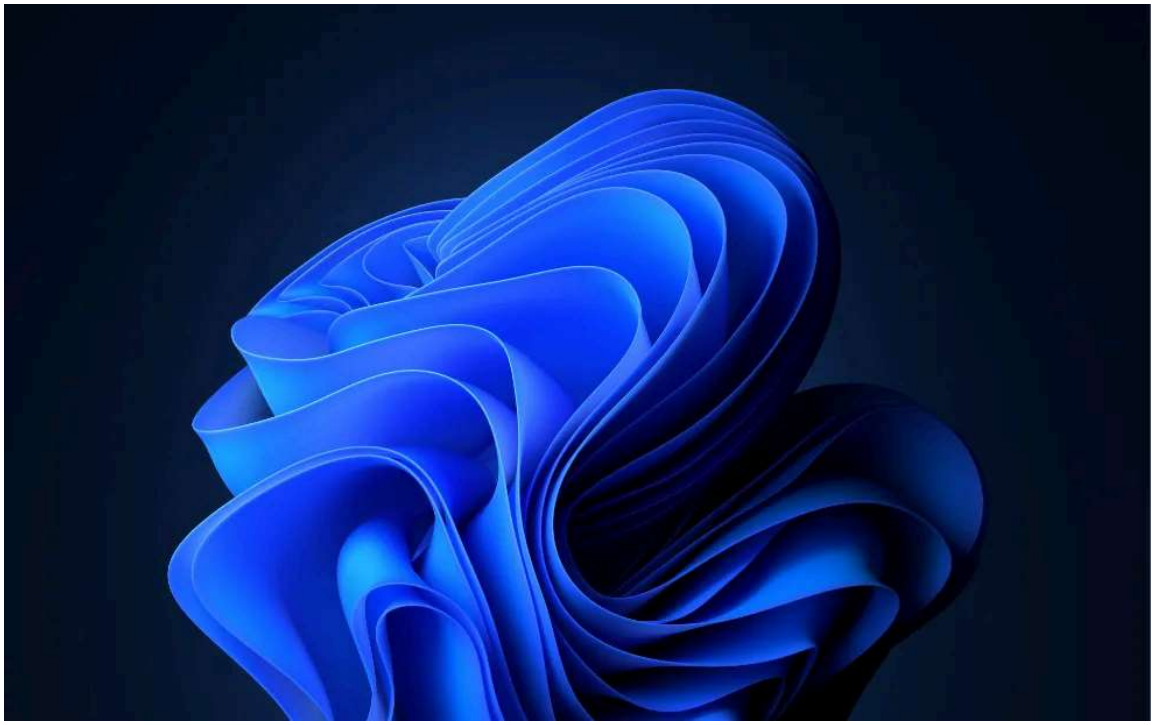
出品 | CSDN（ID：CSDNnews）

“盗版 Windows 11 要凉了？”

最近，一则关于微软加强 TPM 安全机制的消息在技术社区引发热议。不少用户看到标题后第一反应是：**微软是不是终于要动真格了**，准备利用 TPM 芯片检测盗版系统，**让那些没有购买许可证的 Windows 11 直接失效？**

是，但也不全是：微软确实宣布了一项新的安全升级——KMS Hardware-Secured（硬件安全保护的 KMS），要求 Windows 批量授权环境中的 KMS 服务器利用 TPM 进行硬件身份验证。

不过，**这项变化针对的并不是普通用户电脑上的盗版 Windows，而是企业内部部署的 KMS 激活服务器。**



01

TPM + KMS，解决企业授权体系 Bug

这场误会，最初源于微软上周发布的一份技术文档。

WINDOWS IT PRO BLOG WINDOWS IT 专业人士博客 3 MIN READ

Strengthening Key Management Service - (KMS) with Hardware-Based Trust

利用基于硬件的信任机制加强密钥管理服务 (KMS)

Monika_Kumar 莫妮卡·库玛 MICROSOFT 微软

Jul 22, 2026 2026年7月22日

For years, organizations have relied on Microsoft's Key Management Service (KMS) to activate Windows devices at scale. While KMS helped enable broad deployment scenarios, modern organizations increasingly require stronger assurances around device identity and activation integrity. Microsoft has continued to enhance activation capabilities with innovations that leverage hardware-backed validation to provide stronger protection against activation misuse and improve trust in device identity.

多年来，各组织机构一直依赖微软的密钥管理服务 (KMS) 来大规模激活 Windows 设备。虽然 KMS 帮助实现了广泛的部署，但现代组织机构越来越需要更强大的设备身份和激活完整性保障。微软不断通过创新来增强激活功能，利用硬件支持的验证来提供更强大的保护，防止激活被滥用，并提高对设备身份的信任度。

As attackers have exploited fake or cloned KMS servers, organizations face increased compliance and licensing risk. Microsoft is now further strengthening defenses with KMS Hardware-Secured, which uses Trusted Platform Module (TPM)-based attestation to help verify that a KMS host is running on trusted hardware before it can activate Windows devices.

由于攻击者利用伪造或克隆的 KMS 服务器，企业面临着日益严峻的合规性和许可风险。微软现通过 KMS 硬件安全技术进一步加强防御，该技术利用基于可信平台模块 (TPM) 的认证机制，在 KMS 主机激活 Windows 设备之前，验证其是否运行在可信硬件上。

由于 Windows 11 在支持的设备上本就硬性要求 TPM 2.0，不少媒体就把这两件事情联系到了一起：一边是 Windows 11 对 TPM 的要求；另一边是微软宣布 KMS 引入 TPM 验证。于是，一些报道便得出了一个**看似合理、实则错误**的结论：

“微软将利用 TPM 芯片识别盗版 Windows 11，并阻止盗版激活。”

实际上，微软此次升级针对的是 KMS（Key Management Service，密钥管理服务）。

对于普通消费者来说，Windows 激活通常依赖购买的产品密钥或者绑定微软账号的数字许可证；但对于大型企业、政府机构、学校等组织来说，管理成千上万台电脑时，不可能每台设备单独输入密钥——因此，这些机构通常会部署自己的 KMS 服务器。

简单来说，**KMS 的作用类似于企业内部的“授权中心”**：员工电脑向 KMS 服务器请求激活 → KMS 服务器确认企业拥有合法批量授权→ 然后为大量 Windows 设备提供激活服务。

这种模式极大降低了企业管理成本，可问题也随之出现：**如果攻击者创建一个“看起来像真的”KMS 服务器**，并让它接入企业网络，就可能偷偷响应激活请求，**为企业中没有购买授权的设备提供 Windows 激活。**

也就是说：攻击者都不用破解 Windows 本身，只需假装成一个“合法的授权服务器”——微软此次推出的 KMS Hardware-Secured，就是为了堵住这个Bug。

// 02

KMS 服务器要证明：“我是我，且没被动过手脚”

据官网介绍，在新机制下，KMS 主机必须借助 TPM 完成硬件级身份验证。

微软要求 KMS 服务器证明两件事情：

- 第一，它是真实存在的合法硬件。TPM 会生成并保存设备身份信息，微软可以检查该身份是否符合预期。
- 第二，它没有被恶意篡改。TPM 可以验证服务器平台状态，确保运行环境没有被攻击者修改。

如果 **KMS 服务器无法通过其中任意一项验证，那它将无法继续向设备提供 Windows 激活服务。**

微软表示，这种机制可以防止克隆企业 KMS 服务器、伪造激活请求响应、非授权设备通过假服务器获得 Windows 激活，同时也为未来更加严格的安全合规要求做准备。

// 03

企业 IT 管理员可提前检查

根据微软说明，如果企业使用的是物理 KMS 主机，需要确认两件事情：服务器是否通过 Windows Server Catalog（Windows Server 目录）认证；TPM 芯片是否已经安装并启用。至于运行在虚拟机环境中的 KMS 主机，目前微软还没有完全公布虚拟 KMS 环境下的具体要求。

对于企业 IT 管理员来说，这项变化也不会立即生效。微软计划从 2026 年 8 月开始，让 Windows Server 2025 显示 KMS 硬件安全功能的准备状态。在此之前，管理员可以提前检查自己的 KMS 环境是否满足要求。

例如，在管理员权限 PowerShell 中运行：

```
Get-TpmSupportedFeature -FeatureList “Key Attestation”
```

如果设备支持该功能，系统会返回相关信息，说明硬件具备 TPM 认证能力。

此外，还可以在 KMS 主机上执行 slmgr /dlv，以查看当前状态。同时，Windows 事件查看器中的：Applications and Services Logs > Key Management Service，也会记录对应状态。

不过需要注意：**这些提示只是帮助企业提前准备，并不会立即阻止激活，现有 KMS 部署仍可以正常工作。**真正强制执行，要等微软未来发布新的 Windows Server LTSC（长期服务版本）之后。

04

所以，普通 Windows 11 用户会不会被影响?

那么，普通用户最关心的问题来了：**自己的 Windows 11 会不会突然无法激活?** 答案是：**不会。**

一些媒体认为：去年微软封堵了 KMS38，这次又升级 KMS 安全机制，说明微软正在全面围剿“盗版 Windows”——**但实际上，两者并没有直接关系。**

此次 TPM 验证机制检查的是企业用于批量授权的 KMS 服务器：它不会扫描用户当前正在使用的电脑，也不会验证家庭版 Windows 11 是否通过 TPM 激活，微软也没有为零售版 Windows 11 引入新的 TPM 授权检查机制。

目前常见的正版激活方式，包括Windows 零售版产品密钥和微软账号绑定数字许可证，都不会受到影响。

事实上，**当前大量盗版 Windows 激活工具甚至已经绕开 KMS。**

例如 HWID 激活，它会模拟合法数字许可证流程，将设备硬件信息关联到微软激活体系，让系统表现得像拥有正版授权，整个过程不需要 KMS 服务器。另一种方式 TSforge，则是直接修改 Windows 软件保护平台中的授权数据文件——通过伪造授权信息，系统会认为自己已经完成激活，它同样也不依赖 KMS。

因此，**从技术角度来看：微软此次的 KMS Hardware-Secured 并不能直接终结现有盗版 Windows 激活方式。**

05

微软为什么没有大规模追击个人盗版用户?

可能有不少人疑惑：既然微软有能力通过 TPM 加强企业授权安全，为什么不直接利用类似技术打击所有盗版 Windows?

原因其实很简单：**微软当然希望用户购买正版许可证，但追踪每一个个人用户并采取法律行动，成本要远高于收益。**

目前 Windows 11 Home 官方售价约为 139 美元，Pro 版本约为 199 美元。对于购买高价电脑的用户来说，这笔费用可能可以接受；但对于自己组装低价 PC，或购买入门级笔记本的用户来说，硬件之外再额外支付一套操作系统费用，确实是一笔不小的开支。

这也是一些盗版激活工具多年后依然存在的原因。

此外，微软如今的商业模式也早已不只是依靠 Windows 授权收入：无论用户是否购买 Windows 许可证，微软还可以通过 Microsoft 365、OneDrive、Copilot、MSN 服务广告等生态服务获得收益。

过去几年，Windows 11 也因此被不少用户吐槽“广告越来越多”。微软后来承认推广内容确实过多，并开始减少部分系统内置推荐，例如默认关闭部分 Widgets 和 MSN 信息流广告。

所以，**比起用户是否支付了一次 Windows 授权费用，微软更关注的可能是：用户是否一直留在 Windows 生态中。**

参考链接：https://www.windowslatest.com/2026/07/27/you-heard-wrong-microsoft-isnt-ending-pirated-windows-11-with-tpm-and-the-new-rule-only-affects-enterprise-servers/

力挺中国AI模型，黄仁勋70分钟访谈回应AI争议：优秀开源模型应该被使用、英伟达的成功可能复现、AI消灭一半岗位是胡说八道

亲历 AI 提效的真实混乱：一个 PR 改了 50 万行代码、产研关系差点崩了

首个鸿蒙 PC 开源AI统一工作台JiuwenSwarm，重塑桌面生产力！


早鸟票
限时开售！
GOSIM
SHENZHEN
2026
全球开源 AI 大会
EARLY BIRD
早鸟票开售
10 月 16—17 日
深圳
大会亮点
150+
全球讲师
2000+
全球开发者
Agentic AI / 开源大模型 / 开源机器人 /
边缘智能体 / 智能体操作系统
Keynote + Workshop +
Hackathon + AI Vision Forum
锁定你的
开源 AI 盛会席位！
扫码购票

阅读原文