精选快讯　软件快讯　2026年11月15日 22:04

Cursor披露Fireworks AI密钥泄露致后门Claude Code扩展植入市场缓存

要点

- Cursor披露其10月安全漏洞源于Fireworks AI泄露的访问密钥。
- 攻击者利用窃取的凭证，将修改后的Claude Code软件包植入Cursor VS Code扩展市场的缓存中。
- Cursor表示，最多5,000名请求特定缓存版本的用户在约11小时内可能收到了恶意构建版本。

Cursor披露其10月安全漏洞源于Fireworks AI泄露的访问密钥。该被盗密钥提供了对共享存储桶的只读访问权限，攻击者借此窃取历史编码代理记录并发现更多凭证。Cursor于11月13日发布的更新确认，供应商暴露与10月29日发现的恶意软件包直接相关。

攻击者利用窃取的凭证，将修改后的Claude Code软件包植入Cursor VS Code扩展市场的缓存中。受影响版本为Windows和macOS平台的Anthropic.claude-code 2.1.312及2.1.313。技术分析显示，注入的JavaScript在扩展加载时运行，收集主机详情，添加标记为svc-telemetry的SSH密钥，并尝试建立反向SSH隧道。此外，恶意代码还通过macOS LaunchAgent和Windows计划任务实现持久化。

Cursor表示，最多5,000名请求特定缓存版本的用户在约11小时内可能收到了恶意构建版本。数据显示，少于0.05%的用户编码代理痕迹及少于0.01%的客户API凭证暴露。Cursor强调Anthropic未发布这些软件包，Open VSX也未托管该恶意软件。目前，Cursor已撤销供应商访问权限、轮换内部凭证、重建扩展市场并扩大安全扫描，认为事件已得到控制，最后攻击者活动已于11月1日被阻止。

报道来源：cybersecuritynews

来源网站：https://www.inews.today/