预警编号：YJ-2017034

恒安嘉新

关于惠普笔记本电脑键盘驱动

存在记录器代码调试漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 12 月 11 日

1 漏洞描述

近期，互联网爆出惠普笔记本电脑键盘驱动存在记录器代码调试漏洞，攻击者利用该漏洞可以监视用户并获取敏感信息。恶意软件的开发者可以通过修改注册表键值来启用键盘记录行为，并使用原生本地内核签名工具监视用户，这些工具无法被安全产品检测到。漏洞危害程度为高危(High)。

2 影响范围

惠普已经发布了一份受影响笔记本电脑的列表，包括固件更新的链接，共有 475 个型号，包括 303 个用户笔记本和 172 个商业笔记本移动客户端和移动工作站。

受影响的产品系列包括 HP's 25*, mt**, 15*, OMEN, ENVY, Pavilion, Stream, ZBook, EliteBook 系列，以及 Compaq 产品。

详情请参考惠普官网链接：https://support.hp.com/us-en/document/c05827409。

3 漏洞原理

键盘记录代码出现在 SynTP. sys 文件中，是“Synaptics”触摸板驱动程序的一部分，它可以驱动一些 HP 笔记本模型。默认情况下，日志是禁用的，但可以通过设置注册表值来启用，注册表键为:

HKLM\Software\Synaptics\%ProductName%HKLM\Software\Synapt

ics\%ProductName%\Default。

4 修复建议

惠普已经发布了数百个笔记本的驱动程序更新 ,以删除攻击者可能作为键盘记录器组件被滥用的调试代码。

详情请参考官网链接 : https://support.hp.com/us-en/document/c05827409