



Vista的抵御缓冲区溢出攻击技术研究

<http://www.firstlight.cn> 2010-05-01

缓冲区溢出攻击是一种在互联网时代被广泛利用并危害严重的主要攻击方式。分析了缓冲区溢出攻击的基本原理，总结了缓冲区溢出攻击的关键步骤，并研究分析了Windows Vista的抵御缓冲区溢出攻击的四种关键技术，包括地址空间配置随机化(ASLR)、数据执行保护(DEP)、GS栈保护和安全(structured exception handling, SEH)等技术；最后对Windows Vista抵御缓冲区溢出的整体效果进行了分析，指出了Vista仍然不能完全抵御缓冲区溢出攻击。

[存档文本](#)