计算机应用 2008, 28(9) 2252-2254 DOI: ISSN: 1001-9081 CN: 51-1307/TP

论文

基于Fuzzing的ActiveX控件漏洞发掘技术

吴毓书 周安民 吴少华 何永强 徐威

四川大学 四川大学 四川大学 四川大学

摘要：

Fuzzing是一种有效的自动化的漏洞发掘技术,基于Fuzzing漏洞发掘思想，结合对ActiveX控件的研究，设计并实现了一个Windows系统下的ActiveX控件漏洞发掘平台，并改进了Fuzzing数据产生方案。通过对某些第三方软件安装的控件进行测试，发现了两个已知和一个未知的漏洞，提高了漏洞发掘效率。

关键词： ActicvX控件 漏洞 漏洞挖掘 Fuzzing技术

ActiveX vulnerability exploiting technique based on Fuzzing

Abstract:

Fuzzing is an automated vulnerability exploiting technique. A vulnerability exploiting approach based on Fuzzing and the technical details of ActiveX was proposed. A fuzzer was designed, and effective implementation of data generation was advanced. By testing some third-part software s ActiveX controls, one unreleased and two known vulnerabilities were discovered and the efficiency of the ActiveX fuzz was improved.

Keywords: ActiveX controls vulnerability vulnerability exploiting Fuzzing technique

收稿日期 2008-04-03 修回日期 2008-05-27 网络版发布日期

DOI:

基金项目:

通讯作者: 吴毓书

作者简介:

参考文献：

本刊中的类似文章

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码	2906