ActiveX 漏洞分析与防御策略研究

贺才良,周安民,刘 亮
(四川大学 信息安全研究所,四川 成都 610064)

摘 要: ActiveX 漏洞是一种常见的漏洞,其近年来又有回升的趋势。由于 ActiveX 控件通常与 IE 浏览器结合使用,使得 ActiveX 漏洞几乎等同于 IE 本身的漏洞,因此其危害性极大。通过细致分析 UUSee 网络电视 UUPlayer.ocx 控件缓冲区溢出漏洞,剖析了 ActiveX 溢出漏洞的形成原因,然后基于开发者和终端用户的角度,总结出了有效针对 ActiveX 控件漏洞的安全防御策略。

关键词: ActiveX 控件;溢出;攻击;防御
中图分类号: TP3 **文献标识码**: A **文章编号**: 1674-7720(2012)04-0060-04

ActiveX vulnerability analysis and defense strategy

He Cailiang, Zhou Anmin, Liu Liang
(Institute of Information Security, Sichuan University, Chengdu 610064, China)

Abstract: ActiveX vulnerabilities are common vulnerabilities, which has a rebounding trend in recent years. As ActiveX controls are often used in combination with IE, ActiveX flaws are almost equivalent to vulnerabilities of IE, resulting their big harm. In this paper, a detailed analysis of UUPlayer.ocx control buffer overflow vulnerability of UUSee network television analyses the causes of the ActiveX buffer-overflow vulnerability, and then from the developers and end-user point of view, summed up effective defense strategies for ActiveX controls vulnerabilities.

Key words: ActiveX control; overflow; attack; defense

微软公司在 1996 年开发了 ActiveX 控件技术,它是在组件对象模型(COM)的基础上发展而来的。ActiveX 控件的诞生与使用,大大扩展了 IE 浏览器的功能,使得 IE 浏览器处理 Web 文件的能力大大增强。

随着 ActiveX 控件的应用越来越多,ActiveX 漏洞曝光也从未间断。自 2006 年开始每年都有大量的 ActiveX 漏洞曝光,其中大部分是高危漏洞,各种利用 ActiveX 漏洞的恶意软件、木马、病毒随处可见,其引发的安全问题不容忽视。近年来 ActiveX 漏洞又有回升的趋势,2011 年 1 月~10 月已公布的 ActiveX 漏洞就已经达到了 89 个[1]。在这些数据当中还不包括未曝光和未被统计的漏洞,ActiveX 漏洞的严重程度可见一斑。因此针对 ActiveX 控件的安全研究十分地关键。

1 UUSee 网络电视 UUPlayer.ocx 控件漏洞逆向分析

2011 下半年,UUSee 网络电视频频爆出 ActiveX 控件漏洞,灰帽子实验室在 6 月 2 日曝光了 UUSee 的 UUPlayer.ocx ActiveX 控件中 DoCmd 函数存在缓冲区溢出漏洞[2]。由于 UUSee 网络电视拥有庞大的用户群,故该漏洞属于"高危"型漏洞。鉴于该漏洞的典型性,本文以此为例对 ActiveX 漏洞进行逆向分析,调试的环境如表 1 所示。

表 1 UUPlayer.ocx 控件漏洞调试环境

软件	版本
调试器	OllyDbg V1.0
浏览器	Internet Explorer 7
操作系统版本	Windows XP SP3
UUPlayer.ocx 版本	6.0.0.1

用 OllyDbg 附加 IE 进程并运行,用 IE 打开 POC 文件。程序崩溃,OllyDbg 捕捉到一个访问异常,EIP 寄存器指向了一个非法地址。采用栈回溯的方法在地址 0x73D47AC1 下硬件执行断点。通过"跳过-异常-进入"方法跟踪到调用漏洞函数指令处:

```
0x73D47F2A    FFD0    call eax
```

发现 eax 指向 UUPlayer 这个控件的地址空间,观察此时的堆栈,一个可疑字符串出现在栈顶作为 CALL EAX 的调用参数,跟进此函数。以下列出了该函数中关键的反汇编代码段。

关键代码段 1：

```
02EB4580    81EC 84000000    sub esp,84
                                    //开辟 132 B 栈空间
02EB4586    83C9 FF          or ecx,FFFFFFFF
02EB4589    33C0             xor eax,eax
02EB458B    8D5424 04        lea edx,dword ptr ss:[esp+4]
…
02EB45A1    8BF7             mov esi,edi
                                    //源字符串地址
02EB45A3    8BFA             mov edi,edx
                                    //目的地址指向栈内
02EB45A5    8D5424 10        lea edx,dword ptr ss:[esp+10]
02EB45A9    C1E9 02          shr ecx,2
                                //开始从源地址复制字符串到栈内
02EB45AC    F3:A5            rep movs dword ptr es:[edi],
                                    dword ptr ds:[esi]
…
02EB45B6    F3:A4            rep movs byte ptr es:[edi],
                                    byte ptr ds:[esi]
```

这部分代码首先在栈内开辟 0x84(132 B)的栈空间，然后将参数所指字符串复制到开辟的栈空间里。从代码可以看出，在复制之前没有检查字符串的长度，只要传入的字符串长度超过开辟空间的大小就会造成溢出，实验溢出示意图如图 1 和图 2 所示。

图 1 溢出前的栈空间

图 2 溢出后的栈空间(1)

从图 1、图 2 可以看出，传入的字符串刚好淹没了返回地址。

关键代码段 2：

```
02EB45B8    BF 5CD3EB02      mov edi,
                                    UUPlayer.02EBD35C
02EB45BD    83C9 FF          or ecx,FFFFFFFF
02EB45C0    F2:AE            repne scas byte ptr es:[edi]
02EB45C2    F7D1             not ecx
…
02EB45D3    4F               dec edi
02EB45D4    C1E9 02          shr ecx,2
02EB45D7    F3:A5            rep movs dword ptr es:[edi],
                                    dword ptr ds:[esi]
…
02EB45E3    F3:A4            rep movs byte ptr es:[edi],
                                    byte ptr ds:[esi]
```

这部分代码的功能是将字符串“\x0a\x00”(换行符)追加到上个字符串末尾，连接后的结果如图 3 所示。返回地址恰好被覆盖成了 0X0A3F2C3F，可以通过堆喷射技术将此地址所在的区域布置成含有 shellcode 的内存块[3]，当函数返回时就会跳到 shellcode 附近，然后堂而皇之地执行 shellcode。

图 3 溢出后的栈空间(2)

经过逆向分析，整个函数的大致功能如下：将传入的字符串写入到栈内的缓冲区，然后在其末尾追加换行符，最后将整个字符串写入到某个文件中。漏洞产生的原因是 DoCmd 方法没有验证字符串参数的长度，导致溢出。将此漏洞和网马技术结合起来构造恶意网页，攻击者就可以在网站上挂马了。Windows 用户如果安装了漏洞版本的 UUSee 网络电视软件，且没有修复漏洞，在用 IE 浏览挂马网页时就会遭受攻击。由于 UUSee 网络电视用户众多，ActiveX 漏洞利用的成功率相当高，因此该漏洞的危害是很严重的。

2 ActiveX 攻击及防御策略

2.1 ActiveX 攻击方式

网络钓鱼是攻击者利用 ActiveX 漏洞实施攻击的主要手段，攻击原理如图 4 所示[4]。攻击者先利用 ActiveX 漏洞构造一个恶意网页，再以邮件的方式将链接发送给受害者。受害者使用 IE 浏览器浏览该网页后，漏洞被触发，嵌在网页中的连接攻击者主机或者服务器功能的 Shellcode 被执行。之后攻击者给受害者主机上传木马。木马盗取用户信息后发送给攻击者或者上传至服务器，

图 4 网络钓鱼原理示意图

攻击者再从服务器查看受害者的信息。

根据 ActiveX 控件的来源可以将 ActiveX 漏洞攻击分为两大类：(1)攻击者提供恶意的有漏洞的 ActiveX 控件让用户下载并安装，然后利用该 ActiveX 控件的漏洞实施攻击；(2)攻击者利用第三方软件有漏洞的 ActiveX 控件实施攻击。具体来讲又可细分为三种情形，如表 2 所示。

表 2 利用第三方控件的三种攻击方式对比

第三方控件攻击方式	成功率	危险性
0day 漏洞	极高	高危
漏洞公布，没发布补丁	高	高危
补丁发布，用户没修复	较高	中危

2.2 ActiveX 攻击的防御策略

虽然舆论界有许多针对 ActiveX 的苛刻批评，但是现阶段 ActiveX 仍然是 IE 浏览器插件的主要安装手段，这就使得 ActiveX 漏洞在短期内不会消失。因此需要开发者和用户联合起来，采取安全措施积极地去防御 ActiveX 漏洞，尽量将风险降到最低。

2.2.1 开发者的防御策略

开发安全的 ActiveX 控件对于 ActiveX 控件的安全至关重要。开发安全的 ActiveX 控件需要设计者、程序员、测试员三者在整个产品的生命周期内紧密配合，高度关注控件的安全特性。本文针对如何开发安全 ActiveX 控件，总结出了安全开发 ActiveX 控件的基本流程，如图 5 所示。

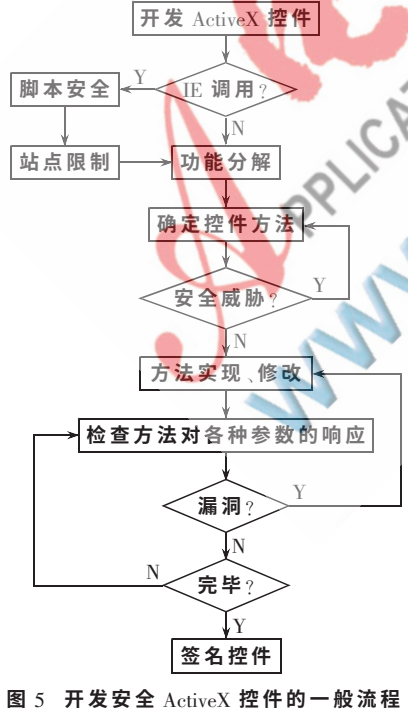

图 5 开发安全 ActiveX 控件的一般流程

设计者需要做的工作有：

(1)综合考虑 ActiveX 控件所带来的好处和存在的隐患，考虑是否可以用其他方法来替代[5]；

(2)该控件是否需要被 IE 调用，如果是就必须将控件声明为脚本安全，采用 ATL 站点限制模板(SiteLock ATL template)将控件进行站点限制，以禁止被别的站点非法使用[5]；

(3)在满足要求的条件下为控件设计最少的功能以减少风险。对照表 3 所示的威胁列表[6]检查各方法是否存在安全威胁。

表 3 ActiveX 控件威胁列表

ActiveX 控件威胁
是否访问本地计算机或者用户信息
是否暴露本地计算机或者网络信息
是否修改或者删除本地计算机或者网络信息
是否引起浏览器崩溃
是否执行不安全的系统调用
是否过度消耗时间或者占用计算机资源
是否可以用于跨站攻击

程序员在编写程序时应该以良好的软件开发实践为导向，编写正确的安全的代码[7]。在控件编写完成并进行完善的测试之后，对控件数字签名，防止被篡改。

测试员应对控件的每个方法进行各种输入参数检测，尤其注意对字符串参数长度和方法内部是否存在整数溢出等进行检测。

2.2.2 用户的防御策略

用户的防御策略主要包括以下三个方面：

(1)提高安全意识，不访问可疑站点和非法站点。

(2)密切关注漏洞安全，及时升级 Windows 系统和安装漏洞补丁，这样可以禁止、修复、移除系统中包含风险的 ActiveX 控件，确保系统安全。对于第三方控件的漏洞，用户可以通过杀毒软件修复或者手动修复。

(3)正确设置 IE 浏览器。

IE 浏览器有许多关于 ActiveX 控件的安全设置，可以阻挡大部分的 ActiveX 攻击。微软在高版本的 IE 浏览器中还增加了多个 ActiveX 安全设置选项，如 IE7 增加了 Opt-in 特性，IE8 增加了 Per-Site 特性，这些特性大大增强了 IE 的安全性能。IE 浏览器存在 4 个安全区域：Internet 区域、本地 Intranet 区域、可信站点区域和受限站点区域，其默认的防御等级分别为：中高、中低、中、高。每个安全域都包含一些设置选项，表 4 所示为几个重点设置选项(只考虑 IE6 及以上的版本)。

Internet 域适用于大部分的站点，防御处于中高等级比较适宜。在特殊情况下，用户需要下载未签名的 ActiveX 控件或者控件没有标记为可安全执行脚本却需要使用脚本，则可以将该站点列入到防御等级较低的可信站点区域内。若用户不信任某个站点，但仍然需要访问它，则可以将其列入到“受限站点区域”。合理设置使用这 4 个区域既可以满足用户的需求又能使 IE 的安全性能得到最大的发挥。

从表 4 还可以看出，高版本的 IE 浏览器支持更多

表 4 安全域 ActiveX 重要设置选项说明

重要设置选项	IE 支持	说明	设置建议
对标记为可安全执行脚本的 ActiveX 控件执行脚本	IE6 及以上	“可安全执行脚本”说明该控件经过了严格的安全测试，设计者可保证控件的安全性，当控件有漏洞时，有安全风险	除受限区域以外的其他 3 个区域“启用”
对未标记为可安全执行脚本的控件初始化并执行脚本	IE6 及以上	未标记为可安全执行脚本，说明控件不是设计为 IE 调用的或者设计者不能保证安全性，脚本调用控件时存在风险	4 个区域都“禁止”，也可根据需要在 Intranet 或者信任区域内“允许”
仅允许经过批准的域在未经提示的情况下使用 ActiveX	IE8 及以上	配合站点限制(SiteLock)功能使用，相应的控件被称为 Per-Site ActiveX	Internet 区域和受限区域“启用”，其他两个域“禁用”
下载未签名的 ActiveX 控件	IE6 及以上	未签名的控件存在较大的安全风险	4 个域都“禁用”，可根据需要在 Intranet 和信任区域内“允许”
允许运行以前未使用的 ActiveX 控件而不提示	IE7 及以上	即 Opt-in 模式，通过第三方软件或者系统安装的 ActiveX 控件在初次运行时是否提示	Internet 区域和受限站点区域“禁止”，其他两个区域“启用”

的 ActiveX 特性选项，其安全性比低版本的要高。另外 ActiveX 控件的安全性还与系统有关。在 Windows Vista 系统和 Windows7 系统中，IE 运行在低完整性(Low-Integrity)保护模式下，当 ActiveX 控件需执行一些中、高完整性操作时会受到用户账户控制(UAC)机制的限制，从而很多在 Windows XP 系统里的攻击方式都会失效。关于这方面的技术读者可参考相关文献资料。

本文主要研究了 ActiveX 控件的安全问题，重点逆向分析了 UUSee 网络电视 ActiveX 漏洞的形成原因及其危害，然后从开发者和用户的角度提出了如何防止 ActiveX 控件漏洞的产生和针对 ActiveX 漏洞攻击的防御策略。实践证明，这些方法和策略能够大大降低 ActiveX 控件漏洞的产生几率，能够有效地抵抗 ActiveX 攻击。ActiveX 控件技术应用相当广泛，其引发的安全问题遍及整个 Windows 系统用户，应当引起开发人员、Windows 用户和安全研究人员的高度重视。

参考文献

[1] 国家信息安全漏洞共享平台.ActiveX 漏洞统计[DB/OL].[2011-10-29].http://www.cnvd.org.cn.

[2] 灰帽首发-UUSee 6.11.0412.1 内存破坏远程执行漏洞[EB/OL].[2011-10-29].http://www.huimaozi.net/?p=122.

[3] 王清，张东辉，周浩，等.0day 安全：软件漏洞分析技术(第 2 版)[M].北京：电子工业出版社，2011：201-203.

[4] LEE D H.Become fully aware of the potential dangers of ActiveX attacks[EB/OL].[2011-10-29].http://www.exploit-db.com/download_pdf/17506.

[5] Designing secure ActiveX controls[EB/OL].[2011-10-29].http://msdn.microsoft.com/en-us/library/aa752035.aspx#ax_repurposing.

[6] 李永成，黄曙光，唐和平.ActiveX 控件中不安全方法漏洞的检测技术[J].微型机与应用，2010，29(6)：62.

[7] ActiveX security：improvements and best practices[EB/OL].[2011-10-29].http://msdn.microsoft.com/en-us/library/bb250471(v=vs.85).aspx.

(收稿日期：2011-10-30)

作者简介：

贺才良，男，1987 年生，硕士研究生，主要研究方向：信息安全，网络通信。

周安民，男，1963 年生，研究员，主要研究方向：网络与信息系统安全。

刘亮，男，1982 年生，硕士，主要研究方向：网络系统与信息安全。