ActiveX 控件中不安全方法漏洞的检测技术

李永成[1],黄曙光[2],唐和平[3]
(1.解放军电子工程学院 研1队,安徽 合肥 230037;
2.解放军电子工程学院 网络系,安徽 合肥 230037;
3.解放军电子工程学院 博士生队,安徽 合肥 230037)

摘 要:针对 ActiveX 漏洞被攻击者频繁地使用来攻击系统和由不安全方法引起的漏洞可能会允许远程攻击者任意地访问本地资源的问题,介绍了检查 ActiveX 控件中不安全漏洞的一般方法,并且使用该方法对几款国内软件进行测试,实验表明该方法能有效挖掘到不安全方法漏洞。

关键词:ActiveX 控件;不安全方法;漏洞
中图分类号:TP309 **文献标识码**:A

Insecure method vulnerability detection in ActiveX controls

LI Yong Cheng[1], HUANG Shu Guang[2], TANG He Ping[3]
(1.No.1 Team, PLA Electronic Engineering Institute, Hefei 230037, China;
2.Network Engineering Department, PLA Electronic Engineering Institute, Hefei 230037, China;
3.Doctor Candidates Team, PLA Electronic Engineering Institute, Hefei 230037, China)

Abstract: ActiveX vulnerabilities are frequently used by attackers. Vulnerability caused by unsafe method may allow remote attackers access arbitrary local resource. The paper proposes a general method of checking ActiveX vulnerability. The effectiveness of this method has been proved by experiments on several domestic software.

Key words: ActiveX controls; insecure method; vulnerability

当今软件开发中,面向组件的编程技术应用越来越广泛。但是,组件的使用使编程人员在软件开发过程中提高效率的同时,一并出现的安全性问题也不可忽视。根据 NVD(National Vulnerability Database)发布的信息,在 2008 年 1 月 1 日至 2009 年 8 月 20 日之间,共发布了 227 条描述为在 ActiveX 控件中引发的漏洞[1]。伴随着网络的普及与基于网络的应用的快速发展,ActiveX 控件在应用的数量上非常巨大,而被收入到 NVD 数据库的只是现存的众多数量的 ActiveX 漏洞中的极少数部分,还有大量的 ActiveX 控件的漏洞由于其软件或控件流行范围的局限而不被 NVD 所关注。

另一方面,伴随着 Windows 2003 和 SP2 在操作系统安全机制上的提升,很多漏洞的利用方式被成功遏制。如今要想在 Windows 系统中找到能够利用的漏洞已经是一件很困难的事情,因此更多的黑客与安全人员把目光转向了第三方软件。近几年,一些知名的软件公司都曾被发现其注册的 ActiveX 控件中存在严重的漏洞,鉴于控件的特点,可以说这些漏洞跟 IE 自身的漏洞没有多大的区别。所以在漏洞挖掘中尽早发现这类漏洞并及时地通知相关厂商,以便做出及时的应对措施显得尤为重要。

1 ActiveX 控件

1.1 什么是 ActiveX

ActiveX 是微软公司在 1996 年引进的,它是在组件对象模型(COM)、对象链接和嵌入(OLE)技术的基础上发展而来[2]。COM 规范是 ActiveX 技术的基础,而 COM 的目的是创建对象和提供接口来实现代码片段的简单复用,而这些接口又能被其他的 COM 对象或者程序调用,ActiveX 就是这项规范与 IE 的结合。这种结合提供了 IE 浏览器与第三方软件的接口,使用 ActiveX 控件可以对 IE 浏览器进行功能扩展,可建立应用程序与网站之间的联系,而这种联系通过浏览器来实现。比如登录一个在线视频网站的时候,网站正是通过浏览器调用 ActiveX 控件打开本地的视频资源。

每一个 ActiveX 控件通常使用 CLSID(Class Identifier)来区别于其他的控件。CLSID 是标识一个 COM 类对象的全球唯一的标识符,它是一个 128 位的随机数。可以从注册表中的 HKEY_CLASSES_ROOT\CLSID 来读出本机已经注册的 CLSID。

ActiveX 控件并不能直接使用,它首先需要在目标机器中进行注册,有很多种方法可以注册控件,除了所有的属于 IE 和操作系统的控件以外,新安装控件可以通过应用程序的安装注册一些控件;还可以通过网页中<OBJECT>标签中的 CODEBASE 属性,从指定位置下载并注册控件;另外通过 DOS 命令 regsvr32 也能手动注册一个控件。

1.2 脚本安全

一个 ActiveX 控件可以被标注为脚本安全 SFS(Safe For Scripting),这意味着 IE 可以通过脚本语言如 JavaScript 或 VBScript 调用控件,并设置或获得它的属性。

有两种方法可以描述一个控件是脚本安全的,第一种方法是使用组件目录管理(Component Categories Manager)来在系统注册表中创建合适的项目。可以通过在这册表编辑器中查看"HKEY_CLASSES_ROOT\CLSID\<control clsid>\Implemented Categories"是否拥有子键 7DD95801-9882-11CF-9FA9-00AA06C42C4。第二种方法是通过实现 IObjectSafety 接口,通过调用 IObjectSafety::SetInterfaceSafetyOptions 方法来确定控件是否为脚本安全[3]。

1.3 KillBit

KillBit 是注册表中的一项,用来标识控件使得在 IE 浏览器或者脚本环境运行时不加载控件。当发现有漏洞的控件时,可以先通过设置 KillBit 来使 IE 在使用默认设置时永不调用 ActiveX 控件。KillBit 是 ActiveX 控件的兼容性标志 DWORD 值在注册表中的特定值 0x00000400。针对 IE 与操作系统的不同,KillBit 在注册表中的位置略有不同[4],可分别表示为:

(1)32 位 IE/32 位 Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\

(2)64 位 IE/64 位 Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\

(3)32 位 IE/64 位 Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\

1.4 控件函数枚举

由于 ActiveX 遵循 COM 规范,因此它也像其他的 COM 控件一样使用相同的方式实现了 COM 接口,COM 接口中很好地定义了一个 COM 组件中所实现的方法和属性。如果控件实现了 IDispatch 或者 IDispatchEx 接口,那么可以通过获得 IDispatch 接口来枚举出控件的方法、参数以及属性等信息。

2 不安全方法漏洞及检测

2.1 不安全方法漏洞

通过分析 NVD 以及 US-CERT(US-Computer Emergency Readiness Team)中关于 ActiveX 漏洞的描述信息,ActiveX 漏洞与其他的漏洞在类型上大致相同,占据漏洞比例绝大部份的是由于缺乏必要输入验证而带来的缓冲区溢出漏洞。另外还包括由于 IE 加载恶意网页而引发的在控件实例化过程中造成的崩溃[5]。本文要提到的不安全方法漏洞,也是在 ActiveX 控件中频频出现的一种漏洞。

如果一个方法被设计是由 IE 调用,那么它应该就被标记为脚本安全,微软在 MSDN 中提供了编写一个安全的控件时对于哪些应该被标为安全提供了指导。但是由于编程人员在安全性上的疏忽,或者根本就不熟悉 ActiveX 的调用机制,一些标记为脚本安全的方法能够轻易地被远程调用者不加任何限制地调用,或者一些本不应该被 IE 所使用的方法错误地被标注上了脚本安全,这些方法给系统带来很大的安全隐患。这类漏洞往往表现为任意的注册表读写、本地文件系统的读写、网络端口的开放,执行文件、敏感信息的泄漏等。由于这类漏洞的利用一般非常简单,因此这类漏洞利用门槛很低,危害性极大。

2.2 ActiveX 控件的检测

2.2.1 威胁建模

威胁建模(Threat modeling)是一个过程,软件开发人员可以使用它来评估,从而减少控件所面临的潜在的威胁[6]。威胁建模来自于软件测试领域,威胁建模的一般步骤是先分解应用程序,建立数据流图,然后识别所面临的威胁,根据威胁识别潜在的漏洞。对于识别潜在的威胁,可以利用 Howard 和 Leblanc 提到的 STRIDE 威胁目录[7]。

但是由于威胁建模一般是建立在拥有软件设计细节的基础上。作为漏洞挖掘工作,常常面临的只是软件的二进制文件形式,很难得到软件设计的源代码,构建完整的数据流图。因此,基于威胁建模的漏洞挖掘工作,很难建立起准确的威胁模型。

2.2.2 基于 STRIDE 指导的渗透测试

渗透测试是指测试人员围绕网络或者系统的安全性展开探测,以发现系统最脆弱的环节[6]。在不安全方法的测试中,函数的参数成为渗透测试的主要入口,分析大量的已公布不安全方法漏洞,发现从暴露的方法名字中,一般就能推断出该方法执行的操作。因为在代码编写时,常常使用有意义的单词来表示方法和参数的名字,如下面的一些例子:

```
LaunchExe(BSTR ExeName)
SaveFile(BSTR FileName,BSTR Url)
Update(BSTR Url,BSTR LocFile)
ExecuteCommand(BSTR Command)
```

这些函数及参数明显地暗示了函数的功能以及所需参数的意义，应当首先尝试使用合适的值来测试这些方法。而利用威胁建模中的 STRIDE 威胁目录可以保证测试的全面性。结合 ActiveX 控件中常常被用来作为功能扩展的方面，应该从表 1 所列的几个方面来测试确定该控件是否包含了不安全方法。

表 1 控件威胁列表

ActiveX 方法潜在威胁列表
是否访问本地或者网络中的计算机信息
是否泄漏了一些敏感信息
是否修改删除本地或网络上计算机的信息
是否执行该方法时会造成不安全系统调用
是否破坏使用该控件的应用程序
是否占用过多的系统资源，如内存、硬盘、网络

2.3 测试的一般步骤

结合 ActiveX 控件的特点及其安全方法机制，图 1 所示的基本流程图提出了不安全方法漏洞挖掘的一般步骤。

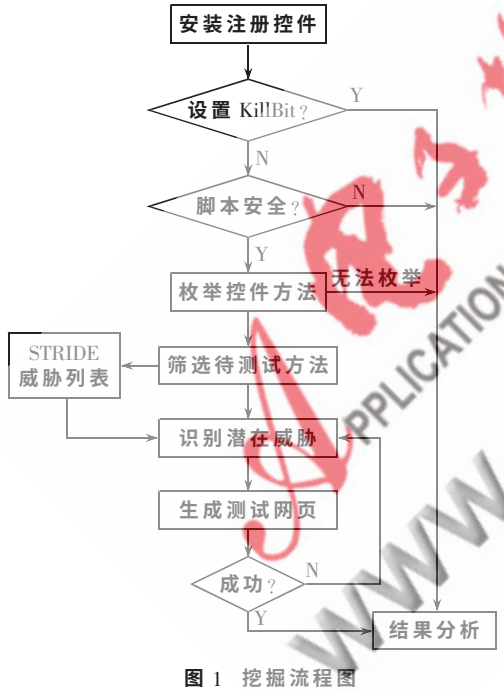

图 1 挖掘流程图

其中，检查是否标注为脚本安全一般先看该控件是否实现了 IObjectSafety 接口，如果没实现则再检查注册表中是否标注脚本安全。在枚举方法中一般可以使用 IDispatch 接口，但是如果控件没有类型库信息，就要借助一些二进制扫描工具如 Strings[8]来搜查 ActiveX 控件的方法和属性。测试网页中，一般使用 <OBJECT CLASSIS="CLSID:"></OBJECT> 标签根据提供的 CLSID 来装载控件，然后可以在脚本语言中对枚举出的函数进行调用。函数调用中要根据测试者之前预测的潜在威胁输入合适的参数，如果测试结果符合预期假设的威胁，则漏洞分析成功，如果测试结果没有实现预期的威胁，则返回查看是否还有其他的潜在威胁可能存在，循环进行测试，直到被测函数被认定不会包含表 1 中所具有的威胁为止。

3 实验及结果分析

本文选取了三款国产软件，分别是 UUsee2008、暴风影音、迅雷看看。将三款软件安装到机器后，分别枚举控件并且检查每个控件的信息，三款软件共在机器上安装新 COM 控件 60 个，其中有 2 个设置 KillBit，10 个被标注为脚本安全。详细信息如表 2 所示，表中可以看到暴风影音没有被标注为脚本安全的控件，在防范不安全方法漏洞方面做得比较好。

表 2 实验结果

软件名称	版本	KillBit	Not SFS	Listing
UUSee	4.0.10	0	11	5
暴风影音	3.9.10	2	34	0
迅雷看看	3.1.0	0	3	5

(1)UUSee 任意文件下载漏洞

软件：UUSee2008

控件名称：UUUpgrade Control

函数：VARIANT_BOOL Update(BSTRbstrLocalINIFile-Name, BSTR bstrRemoteINIURL, BSTR bstrDetailURL, short nMode)

根据函数名字推测可能具有使用远程文件更新本地文件的作用，符合威胁列表中第一条威胁。因此需要编写测试网页对该方法进行测试，测试结果发现存在之前预测的威胁。该漏洞为已公布漏洞，已发布于国内绿盟漏洞数据库上[9]。

(2)系统信息暴露漏洞

软件：UUSee2008

控件名称：UUUpgrade Control

函数：BSTR GetMacID( )

BSTR GetHDID( )

通过分析函数的名字可预测这两个函数可能分别能使远程攻击者得到本地机器的 MAC 地址和硬盘 ID，存在一定的信息暴露危害，测试结果显示符合之前的预测。两个方法存在泄露系统信息漏洞。

软件：迅雷看看

控件名称：DapCtrl Class

函数：long IsFileExist([in] BSTR filePath)

该函数能够根据攻击者指定的文件路径名称，返回该文件是否存在，返回值为 1 表示存在，为 0 表示不存在。这在远程渗透攻击中会给远程攻击者提供帮助。因此存在信息泄漏的危害。

本文只对 ActiveX 控件中的不安全方法漏洞的挖掘方法作了介绍，这种漏洞利用难度较易，危害极大。本文

介绍的方法，只能对单个的方法分别进行测试，但是还有一些控件的方法需要调用属性信息或者其他方法的结果，这种方法对造成的漏洞需要先对控件中的方法属性之间利用数据流分析建立起联系，这是以后研究中需要进一步完成的工作。

参考文献

[1] NVD[DB/OL].[2009-10-01].http://nvd.nist.gov.

[2] WARLORD.ActiveX-Active Exploitation[EB/OL].[2009-10-01].http://packetstormsecurity.org/papers/attack/activex.pdf.

[3] Safe Initialization and Scripting for ActiveX Controls[EB/OL].[2009-10-01].http://msdn2.microsoft.com/en-us/library/aa751977.aspx.

[4] DORMANN W.Internet Explorer Kill-Bits[EB/OL].[2009-10-1].http://www.cert.org/blogs/vuls/2009/07/internet_explorer_kill-bits.html.

[5] DORMANN W,PLAKOSH D.Vulnerability detection in ActiveX controls through automated fuzz testing[R].Pittsburgh:CERT,2009.

[6] ActiveX Security:Improvements and Best Practices[EB/OL].[2009-10-1].http://msdn.microsoft.com/en-us/library/bb250471(VS.85).aspx.

[7] HOWARD M,LEBLANC D.编写安全的代码(第2版)[M].程永敬,译.北京:机械工业出版社,2005:50.

[8] String[CP].[2009-10-01].http://technet.microsoft.com/zh-cn/sysinternals/bb897439(en-us).aspx.

[9] UUSee 网络电视 2008 UUUpgrade ActiveX 控件 Update 方式任意文件下载漏洞[EB/OL].[2009-10-01].http://www.nsfocus.net/vulndb/12075.

(收稿日期:2009-10-28)

作者简介:

李永成,男,1986年生,硕士研究生,主要研究方向:信息安全、软件工程。

黄曙光,男,1960年生,博士生导师,教授,主要研究方向:信息安全、网络仿真。

唐和平,男,1981年生,博士研究生,主要研究方向:信息安全,入侵检测系统。