E:\projectDocuments\1.品牌营销管理\执行\2012\2.Do\3.品牌营销\3.营销实践\1.整合营销\Security+\商标注册\V2\图形+文字\文字+图形1.jpg

网银安全控件

远程代码执行漏洞分析

Content

[背景信息 3](#_Toc420659341)

[危害程度 3](#_Toc420659342)

[分析步骤 3](#_Toc420659343)

[检测方法 3](#_Toc420659344)

[查看IE浏览器安全设置 3](#_Toc420659345)

[检查可信站点区域安全级别 4](#_Toc420659346)

[可能的利用方法 5](#_Toc420659347)

[分析结果汇总 6](#_Toc420659348)

[紧急应对方法 6](#_Toc420659349)

[给银行方面的建议 6](#_Toc420659350)

[给网银用户的建议 6](#_Toc420659351)

[威胁情报 7](#_Toc420659352)

[关于绿盟科技 7](#_Toc420659353)

执行摘要

5月11日，绿盟科技威胁响应中心接报乌云通告，某银行安全控件可导致远程任意代码执行漏洞（WooYun-2015-96339），考虑到互联网金融当前存在较多的安全性问题[[1]](#footnote-2)，并考虑到该漏洞涉及到支付宝安全控件，可能的影响面较大，故迅速展开应急响应工作。

1. 11日，接乌云通告该漏洞情况，启动漏洞分析工作。
2. 11日，对各银行网银安全控件展开分析及检测工作，并给出应对方法。
3. 12日，发布紧急通告，并将分析报告发送给客户及合作伙伴。

如果您需要了解更多信息，请联系：

* 绿盟科技威胁响应中心微博
* <http://weibo.com/threatresponse>
* 绿盟科技微博
* <http://weibo.com/nsfocus>
* 绿盟科技微信号
* 搜索公众号 绿盟科技

背景信息

该问题起源于乌云平台对某银行控件安全问题的一处通报[[2]](#footnote-3)，通报指出，该银行的网银控件会降低网银用户电脑中的安全配置（该配置存在于IE浏览器中）。当这台被降低的电脑访问常规条件下的可信网站时，会执行可信网站要求的任意命令，如果该漏洞被攻击者利用，很容易构造跨站攻击，在用户的电脑上执行任意代码。

危害程度

通俗来说，这个问题可以理解为一台“漏洞放大器”，它自己可能不会造成特严重的危害，但配合上其他漏洞，会放大其他漏洞造成的危害，可以预见的危害有以下几项：

* 该漏洞涉及网银登录页面，以及可能涉及较为及常见的信任网站（比如淘宝、支付宝等），两者的共同用户很多，可能被攻击的范围较大，危害较大；
* 网银出于兼容性及可用性的考虑，可能会降低IE安全性设置，由此动作带来的错误设置可能存在于多家银行；
* 该漏洞是由于网银控件的错误设置，允许在浏览受信任网站时执行任意代码，且没有任何提示，这提升了跨站攻击的威胁程度，用户可能更容易受到伤害；
* XSS跨站攻击本身存在易传播性，配合其他漏洞进行组合攻击，将会进一步扩大影响范围

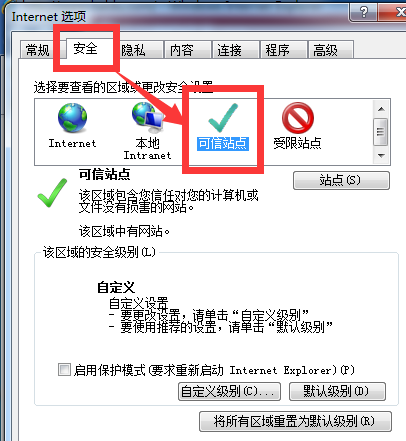
分析步骤

检测方法

为有效应对此漏洞，建议用户尽快通过如下方法检测自己是否已经受到影响。

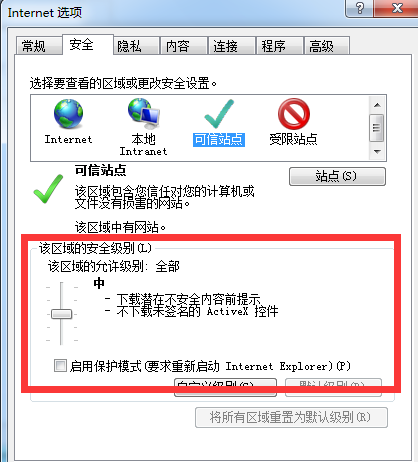
查看IE浏览器安全设置

* “启动IE浏览器，找到并点击“工具菜单”- “Internet选项”
* 在随后出现的对话框中，点选安全标签页
* 在下面第一个窗口中点击“可信站点”图标



检查可信站点区域安全级别

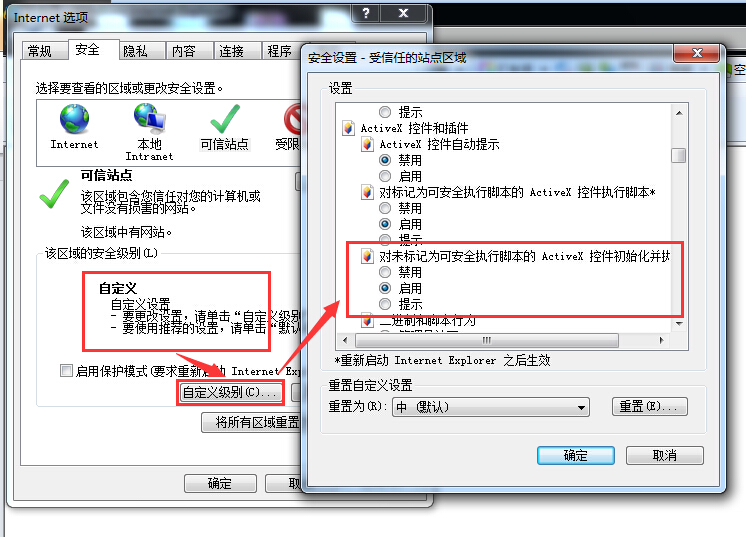
选择该选项后，如果发现红框中的安全级别为“中”，则表明自己所使用的网银控件不存在类似问题，下图是安全情况的样例图。



选择该选项后，如果发现红框中的安全级别为“自定义”，则需要通过如下步骤进一步确定问题：

* 点击“自定义级别”按钮
* 在新弹出的对话框查看“对未标记为可安全执行脚本的ActiveX控件初始化并执行脚本”这一项
  + 如果选择项为“启用”，则表明存在相应问题

下图是存在安全风险的样例图：



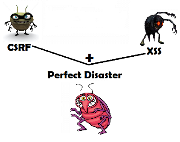
可能的利用方法

通过上面的分析可以看到，此次漏洞的关键在于这个控件错误的设置，打开了“对未标记为可安全执行脚本的ActiveX控件初始化并执行脚本“选项，从而允许执行任意Javascript代码，那么一个典型的XSS跨站攻击可能是这样的：

* 构造一个恶意脚本并将其嵌入URL中，发送给被攻击者
* 被攻击者打开URL，看到还是银行官网，乃至信任域内的任意网站，比如\*.taobao.com
  + 本来这个脚本在本地会受到IE的安全设置的限制无法在执行，默认设置为中级以上
  + 但由于安全控件打开了这道门，恶意脚本已经在后台执行了
* 那么该脚本完全可能在后台下载木马，进而窃取用户的敏感信息，包括授权、信用卡、账号信息等

如果该URL进一步扩散，无论给用户的切身利益，还是对银行的声誉，带来的危害是极其严重的；如果信任域内的网站沦陷，可导致访问该网站的所有用户被挂马，同样是一个一次攻击危害放大的效果。

在《2014绿盟科技互联网金融安全报告》中可以看到，在各种常规漏洞中，XSS是出现频率最多的漏洞类型，占到了13%[[3]](#footnote-4)。其中主要包括反射型XSS和存储型XSS。跨站脚本漏洞可能会导致网页挂马、用户权限被盗用、钓鱼攻击等多种安全风险。



分析结果汇总

通过上面的分析可以看到，该漏洞可能提升现有漏洞的威胁程度，进而引起大规模网页挂马事件，其危害性极为严重，所以绿盟科技技术人员第一时间对8家银行页面进行了检测，发现某银行网银页面均存在控件安全性问题，各行页面详细检测情况截图详见附录。

|  |  |
| --- | --- |
| 银行网银页面安全控件分析结果  某行网银存在控件安全性问题 | |
|  |  |
| 控件所属银行 | 问题存在情况 |
| 中国银行 | 无问题 |
| 农业银行 | 无问题 |
| 中国建设银行 | 无控件 无问题 |
| 某银行 | 存在 |
| 招商银行 | 无问题 |
| 民生银行 | 无问题 |
| 兴业银行 | 无控件 无问题 |

紧急应对方法

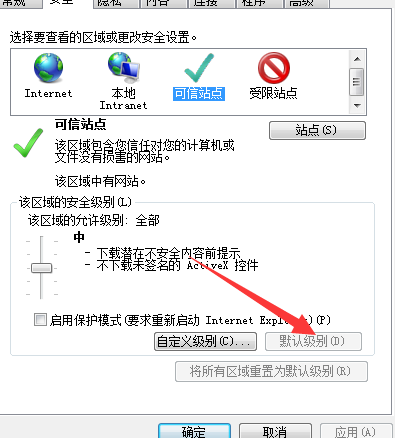
给银行方面的建议

对自己所属银行的控件进行安装审计（审计方法参考检测方法章节），如发现其修改了IE的安全配置，证明该控件存在类似问题。此时应当联系己方开发人员，取消这一修改配置的功能，并发布新版本控件。如控件自身功能有修改IE的安全配置的需求，也要借助其他功能等价编码实现进行该问题规避，重构后发布新版本控件。

给网银用户的建议

普通用户可以先检查自己的浏览器是否存在类似问题，检查方法同样参考检测方法的章节。

如发现自己的控件存在问题，则应将电脑的IE选项手动修复为默认级别（点击“默认级别”这个按钮即可--------在“自定义级别”旁边）。此后，当银行发布新版本控件时，再进行控件更新即可



威胁情报

为及时有效的应对各类网络安全事件，绿盟科技一直与各安全机构保持密切合作，包括乌云及CNCert国家互联网应急中心。从此次安全事件的传播情况可以看到，无论其原理怎样，无论防护方案如何实施，关键在于尽可能快的了解到漏洞信息及相关的情报，以便尽可能快的启动应急响应机制。这无论对于解决传统安全或者APT攻击来说都是重要的手段之一，威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报并持续进行后续服务，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索绿盟科技联系我们，欢迎您的垂询！

关于绿盟科技



北京神州绿盟信息安全科技股份有限公司（简称[绿盟科技](http://www.nsfocus.com/)）成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及Web安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于2014年1月29日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369

1. 2014绿盟科技互联网金融安全报告，<http://www.nsfocus.com.cn/news/201505/915.html> [↑](#footnote-ref-2)
2. 乌云，http://wooyun.org/bugs/wooyun-2010-096339 [↑](#footnote-ref-3)
3. 2014绿盟科技互联网金融安全报告，<http://www.nsfocus.com.cn/report/2014%20NSFOCUS%20Internet%20Finance%20Security%20Report.pdf> [↑](#footnote-ref-4)