安卓微信、QQ自带浏览器UXSS漏洞

北京知道创宇信息技术有限公司

2015-12-26

hei@knownsec.com

（知道创宇404安全实验室）

一、漏洞描叙

在安卓平台上的微信及QQ只带浏览器均使用的QQ浏览器X5内核，在处理ip及域名hostnames存在逻辑缺陷，从而绕过浏览器策略导致UXSS漏洞。

二、POC代码及简单分析

POC.htm的代码如下：

```
<iframe src=‘http://1.1.1.1..qq.com'><iframe>
```

当安卓手机用户使用微信或QQ访问POC.htm时，真实请求并解析执行的是

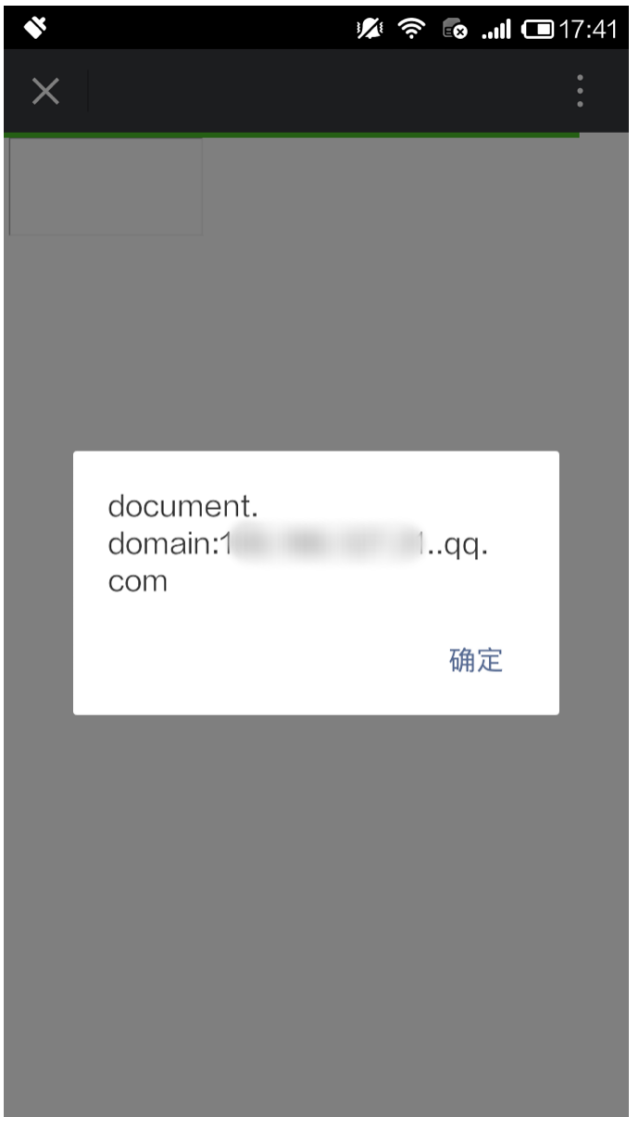
http://1.1.1.1/..qq.com/ 页面代码如下：

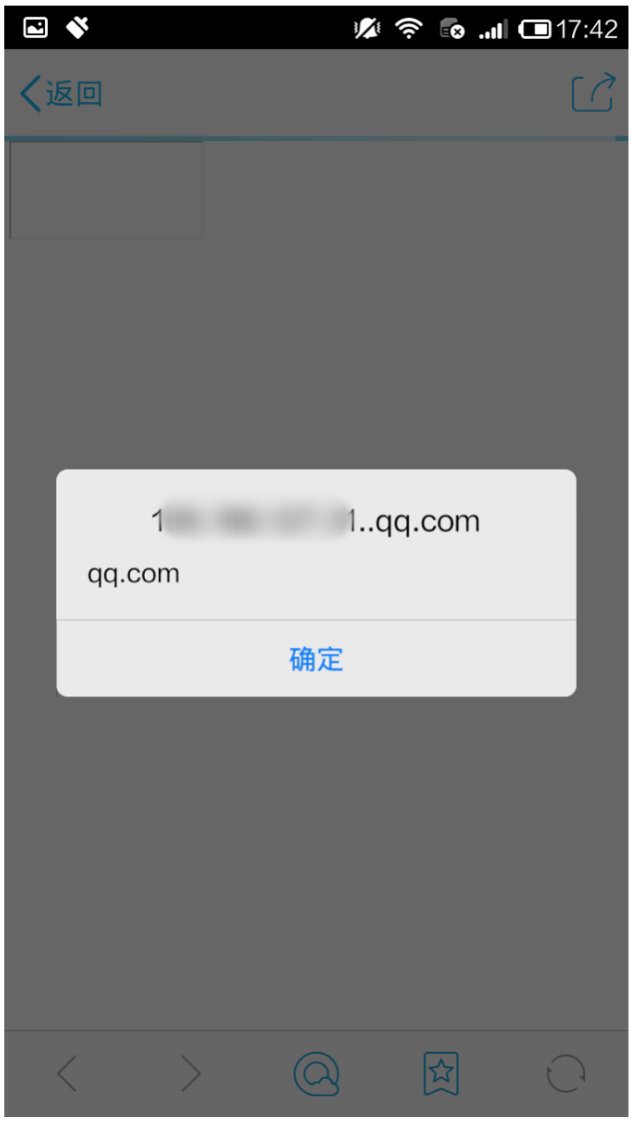
```
<script>
        alert('document.domain:'+document.domain);
        document.domain ='qq.com';
        alert(document.domain);
</script>
```

也就是说当遇到 ip地址+“.”+跟域 的URL自动根据IP地址结构分割URL并访问该IP地址，而浏览器解析的JavaScript代码则按当前的document.URL来处理，会认为当前的document.domain为跟域的子域。

三、漏洞演示

测试POC.htm 微信、QQ扫描或者点击访问URL





注：微信版本号为 6.3.8　QQ版本号为 v6.1.0.2635

四、漏洞利用思路

1、通过设置document.domain来实现跨域。
2、结合flash的crossdomain.xml的设置来进行跨域。
3、利用html5或者其他第三方插件如(jre)等可能实现跨域。

五、可能的影响面及修复建议

最早我发现该漏洞的时候测试安卓QQ浏览器是受到影响的（后面测试失败），所以该漏洞可能影响到其他调用QQ浏览器内核的产品线，所以建议在QQ浏览器X5内核心上修复处理该漏洞。具体修复可以判断处理好IP结构符号”.”。

六、漏洞时间线

2015年10月	发现安卓QQ浏览器受该漏洞影响
2015年12月	发现安卓QQ浏览器不能触发，但微信、QQ等产品能触发
2015年12月26日	漏洞报告提交给TSRC http://security.tencent.com/
2015年12月28日	TSRC确认该漏洞
2016年01月20日	TSRC反馈漏洞已修复
2016年02月29日	对外公布漏洞报告

联系我们

官方网站：http://www.knownsec.com/