# 启明星辰安全产品精确拦截Firefox PDF Reader最新漏洞

## 事件背景

 近日，Mozilla基金会发布一个Firefox浏览器的安全更新，即CVE-2015-4495漏洞，该漏洞存在于Firefox浏览器内置PDF阅读器的pdf.js中，危险级别为：高危。该漏洞允许攻击者绕过同源策略，在本地文件上下文中植入远程执行JavaScript代码，该漏洞的利用代码已经在网络中被大量散播。攻击者们通过该漏洞，可以获得本地文件的读写权限，然后可以进一步将各类恶意代码上传到目标主机上或者从目标服务器上下载系统敏感文件，因此，我们建议使用Firefox火狐浏览器的用户，尽快更新火狐版本（当前最新版本为40.0.2），及时修改用户密码，目前，启明星辰的多款安全产品可以有效检测和精确防御Firefox浏览器最新漏洞所引发的安全事件，并提示广大启明星辰安全产品的用户及时更新产品事件库。

## 漏洞概要

如下是Mozilla官方的安全更新：<https://www.mozilla.org/en-US/security/advisories/mfsa2015-78/>

受影响系统：

Mozilla Firefox < 39.0.3  
Mozilla Firefox ESR < 38.1.1  
Mozilla Firefox OS < 2.2

Firefox PDF reader 在实现上存在安全漏洞，远程攻击者利用此漏洞可绕过同源策略，读取任意文件或获取提升的权限，通过利用这个漏洞，攻击者就可以向PDF阅读器注入一个能够搜索和上传本地文件的脚本。如果目标主机上运行了这个带有漏洞的火狐浏览器，那么这个漏洞就可以允许攻击者从目标计算机的硬盘驱动器之中盗取用户的敏感文件。而且这种攻击方法可以用来攻击Windows和Linux系统平台的用户。

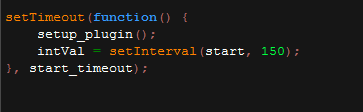
目前网上已经有了攻击者改进的用于Linux平台，Windows平台的攻击脚本，新添加了需要搜集的文件。此外，攻击者还开发了用于Mac OS X操作系统的恶意代码。

在本文中，我们仅对Linux系统下的攻击细节展开介绍。

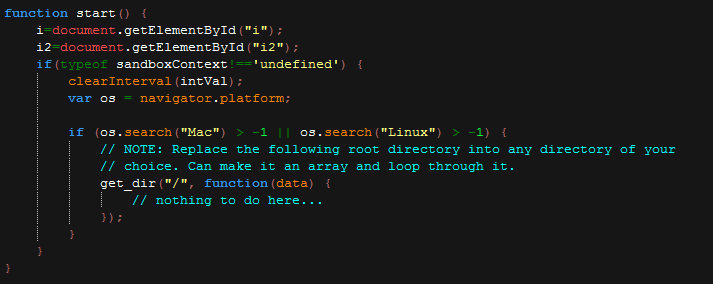
## Exploit恶意脚本分析

Exploit恶意脚本触发后会执行setup\_plugin函数，该函数创建了IFRAME，在IFRAMELoad 函数中，生成了一个空的PDF Blob，当Firefox将要利用内置的PDF阅读器打开这个PDF Blob时，会执行get\_sandbox\_context函数，该函数执行时会在wrappedJSObject中创建一个新的sandboxContext属性。此外,还将一个JavaScript函数写入到了这个sandboxContext属性中。后面的代码将会调用这个函数。同时，利用这些步骤就能够成功地绕过同源策略。

1、恶意脚本首先执行setup\_plugin函数，然后执行start函数

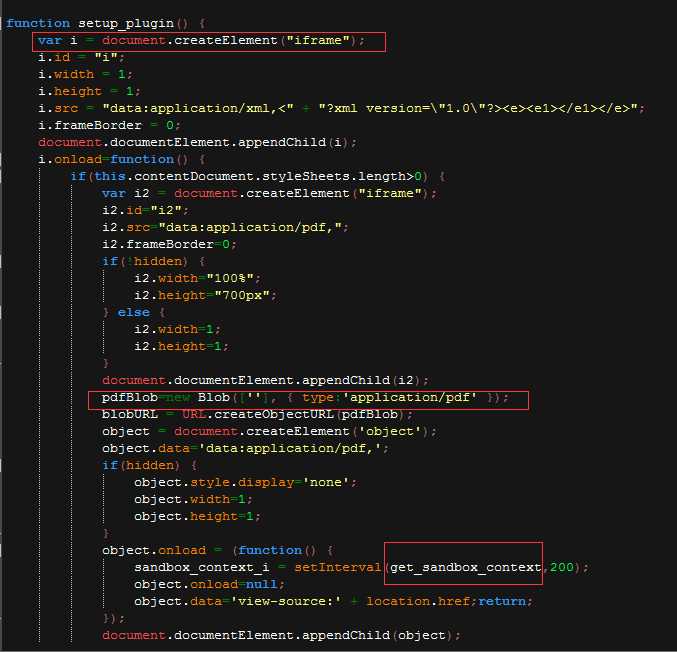


Exploit脚本

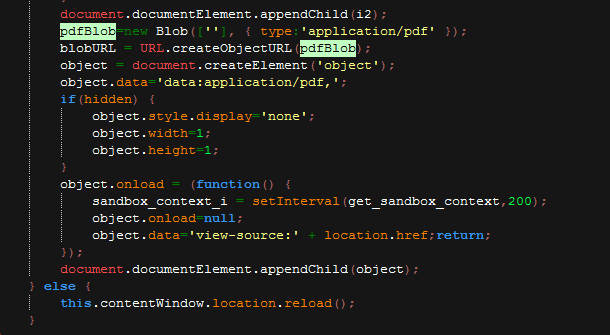


Start函数

2、执行setup\_plugin函数，该函数创建了IFRAME，在IFRAMELoad 函数中，生成了一个空的PDF Blob，当Firefox将要利用内置的PDF阅读器打开这个PDF Blob时，会调用get\_sandbox\_context函数

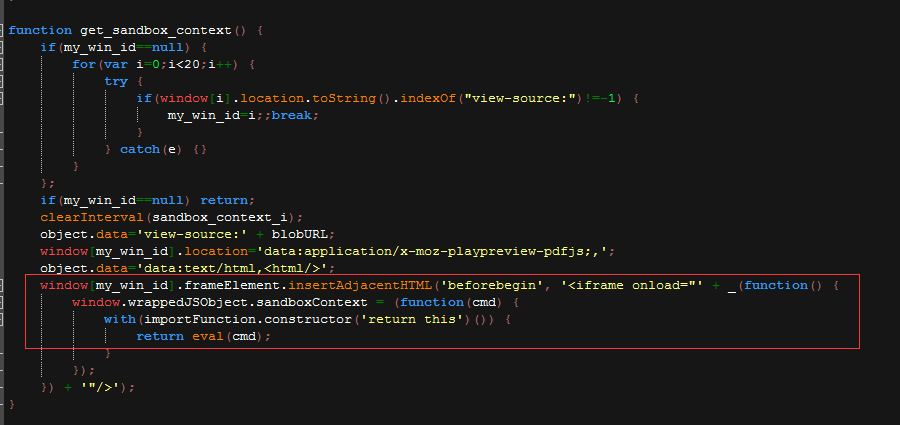


setup\_plugin()函数



空的PDF Blob

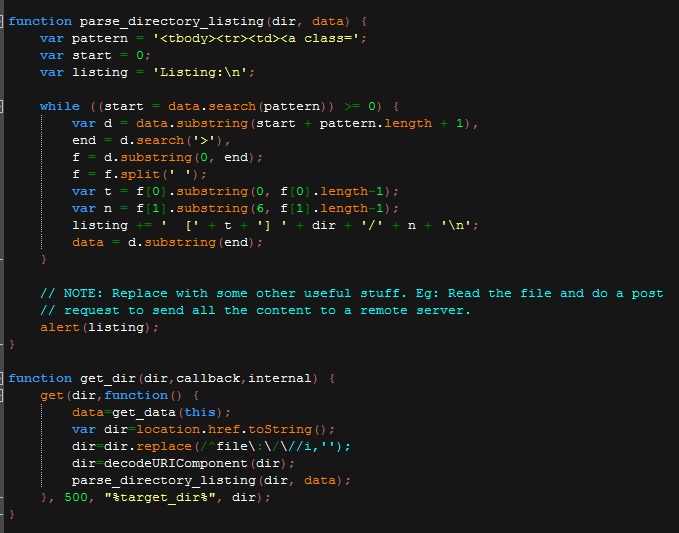
3、get\_sandbox\_context函数执行时，之前生成的IFRAME中会被注入新的代码，在wrappedJSObject中创建一个新的sandboxContext属性。此外,还将一个JavaScript函数写入到了这个sandboxContext属性中。后面的代码将会调用这个函数。同时，利用这些步骤就能够成功地绕过同源策略。



创建sandboxContext属性的代码

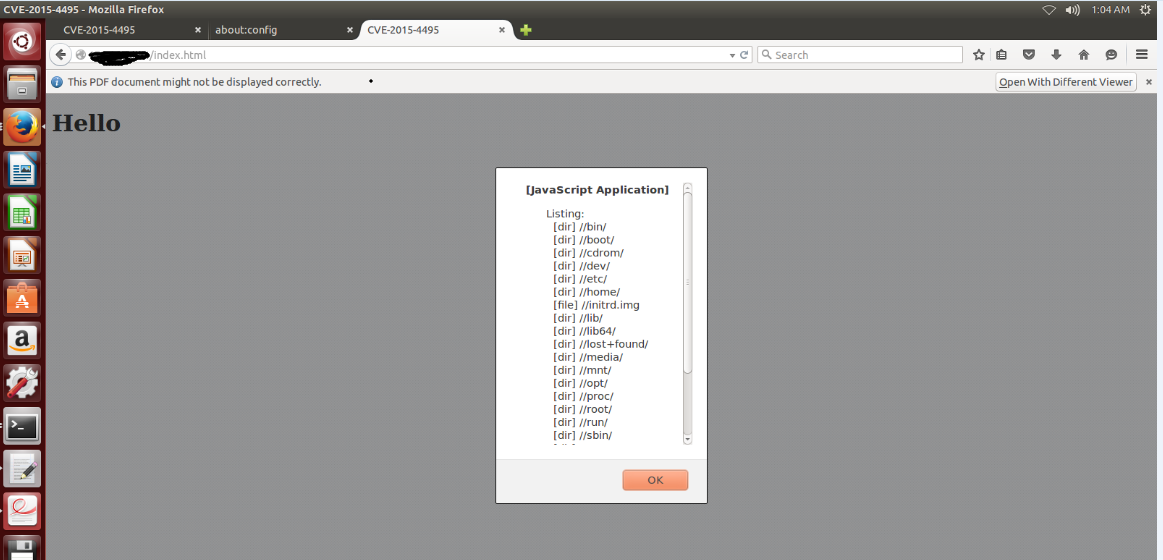
4、Exploit执行Start函数后，将会列出本地文件目录列表，造成信息泄露。

恶意脚本中列出本地文件目录列表的代码如下：



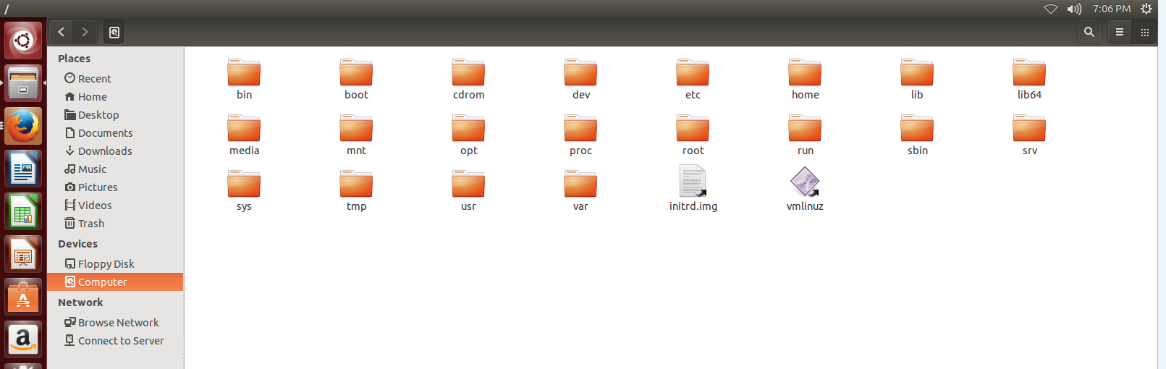
脚本中的目录列表代码

本地目录列表被列出，效果如下图：



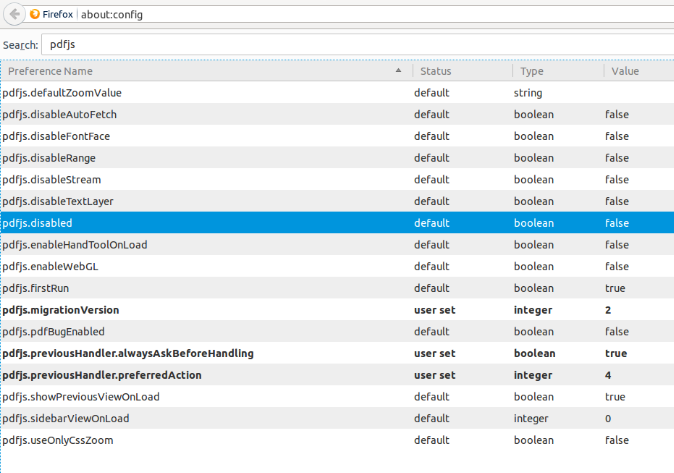
Exploit执行后列出本地文件目录

对比试验机的本地目录文件为：

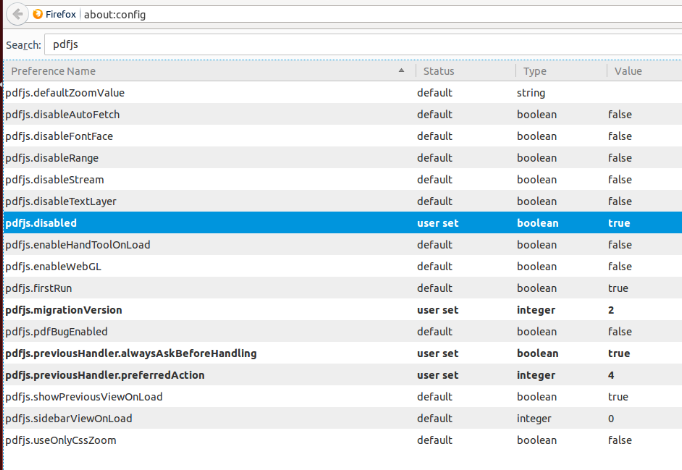


本地目录文件

5、Firefox中内置的PDF阅读器，默认是启用的，所以会引起该漏洞。如果将pdfjs.disabled设为true来禁用Firefox内置的PDF阅读器，则可以避免该漏洞造成的信息泄露。

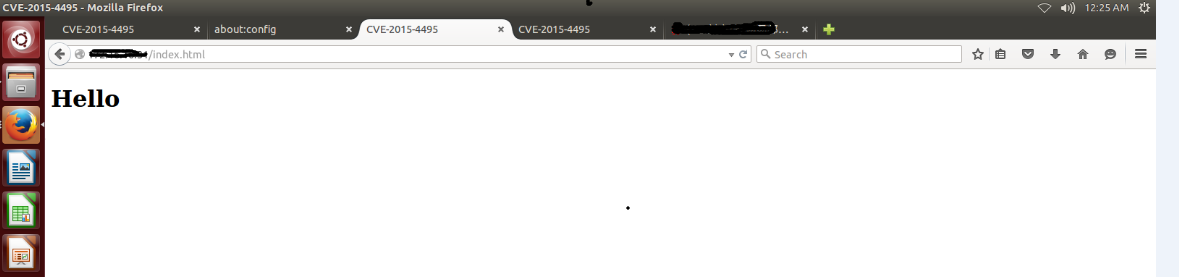


Pdfjs默认启用



禁用Pdfjs

禁用Pdfjs后不再弹窗本地文件列表



禁用Pdfjs后不再弹窗本地文件列表

6、攻击者获得本地文件目录后，然后可以读取任意敏感文件，并将敏感文件发送到远程服务器。

## 产品报警展示：

目前我们的安全产品已经可以报警并防御该漏洞。

入侵检测类系列产品，精确检测Firefox浏览器最新漏洞的截图：



入侵防御类系列产品，精确防御Firefox浏览器最新漏洞的截图：



下一代入侵防御类系列产品，精确检测Firefox浏览器最新漏洞的截图：



## 解决方案

1. 我们建议购买了上述启明星辰信息安全产品的用户，请升级到最新版本的事件库，可准确拦截该样本的漏洞攻击行为。
2. 建议Firefox用户更新到最新版本，当前版本是Firefox 39.0.3版本
3. 用户也可以通过将pdfjs.disabled设为true来禁用Firefox内置的PDF阅读器。