**关于Firefox新版本引入存在专利风险及可选策略分析**

**1．问题背景：**

基于当前openEuler-20.03-LTS相关版本的软件包维护策略，firefox浏览器报出的CVE需要进行及时处理，特别是高分CVE需要及时修复。多数CVE的修复补丁需要升级浏览器来解决。

专利风险：

在调查升级firefox到82版本过程中，发现firefox82使用的流媒体编解码库fdk-acc，经与存在法务公司法务张伟咨询发现存在专利权问题风险，不建议引入，具体如下面截图所示。具体见附件的license，有风险部分如下：





 

 针对firefox存在法务风险的问题，调研引入其他开源浏览器的可能性，如chromium浏览器。

**2．Chromium浏览器引入调研**

**2.1 chromium浏览器及其依赖包在开源、版权、专利方面是否存在问题**

Chromium浏览器是完全开源的，官网为：<https://chromium.googlesource.com/chromium/src>

github.com上托管仓为：

<https://github.com/chromium/chromium>

遵循的开源协议如下：

BSD and LGPLv2+ and ASL 2.0 and IJG and MIT and GPLv2+ and ISC and OpenSSL and (MPLv1.1 or GPLv2 or LGPLv2)

以上所列开源协议已跟公司法务张伟确认不存在版权、专利方面问题，相关license全在白名单列表中。

新引入依赖包[google-noto-fonts](https://117.78.1.88/package/show/home%3Ajeff200902%3Achrome/google-noto-fonts)、[lohit-devanagari-fonts](https://117.78.1.88/package/show/home%3Ajeff200902%3Achrome/lohit-devanagari-fonts)、[lohit-gujarati-fonts](https://117.78.1.88/package/show/home%3Ajeff200902%3Achrome/lohit-gujarati-fonts)、[lohit-gurmukhi-fonts](https://117.78.1.88/package/show/home%3Ajeff200902%3Achrome/lohit-gurmukhi-fonts)、[lohit-tamil-fonts](https://117.78.1.88/package/show/home%3Ajeff200902%3Achrome/lohit-tamil-fonts)这5个字体相关包，全是遵循OFL开源协议的包，不存在法务问题。

**2.2 chromium 在版本发布周期、社区活跃度、用户量、执行效率、安全方面与firefox对比**

（1）发布周期：

Firefox：

延长支持版本（Extended Support Release, 简称“ESR”）是 Mozilla 专门为那些无法或不愿每隔六周就升级一次的企业打造。Firefox ESR 版的升级周期为 42 周，而普通 Firefox 的升级周期为 6 周。

Chromium：

没有发布版本具体周期，看历史版本，也是每月都有stable版本发布。

（2）社区活跃度

Firefox：

在github托管仓看，活跃度不如chromium，差距比较大；

Chromium：

托管仓当前star有7.7k，将近949k commit，19.4 k tags,高度活跃

（3）用户量



（4）执行效率及资源消耗对比



▲ 总测试结果统计，执行速度；

测试结果见：https://www.oschina.net/news/107381/firefox-67-vs-chrome-75-linux-performance



▲ 存消耗对比

测试结果见：<https://www.huxiu.com/article/378248.html>

（5）安全方面对比

 



以上内容，引自绿盟科技《Vulnerability-Development-Trend》，见附件

 

2.3 综述

 在发布周期方面，chromium和firefox较为相似，版本更新都比较快，每月都有更新；在社区活跃度和执行速度方面，chromium 比 firefox都有明显的优势；在资源消耗方面，firefox相比chromium有优势，但在新版本中这种优势越来越小；在用户使用量上，chromium具有压倒性优势；在安全稳定方面，chromium CVE量比firefox多，但chromium用户量大，社区活跃也是CVE量大的一个因素。多方面对比来看，chromium与firefox各有优势，但从社区活跃度和用户量方面，chromium还是更有优势。

1. **Chromium 在openEuler-03、09、主线引入调研**

3.1. chromium浏览器已在openEuler-20.09及master分支环境下，可以正常编译、安装；--已验证

3.2. chromium浏览器在openEuler-20.03相关版本环境，编译不过。注：（因chromium依赖c++的一些新特性，当前已经在gcc上合入了5个patch，chromium合入了2个patch，当前编译不通过）。

3.3.可选的方案：

1. openEuler-20.03 SP1及LTS版本不在处理firefox相关的CVE，也不在升级firefox浏览器（注：参考其他OSV 社区，如CentOS）。openEuler-20.09及主线引入chromium浏览器。
2. openEuler-20.03 SP1版本及LTS版本，同时引入基于gcc9.3编译的chromium和gcc 9.3，并发布版本时声明firefox有CVE漏洞，如果觉得firefox漏洞不可忽略，建议使用gcc9.3和基于9.3编译的chromium浏览器。
3. 继续分析chromium引入的c++新特性和gcc-7.3.0支持的c++特性、寻找chromium引入的且gcc-7.3.0 未覆盖的c++新特性patch，直到chromium浏览器能够正常编译、安装、运行。这个方案带来的就是如果后续还有其他包依赖高版本gcc特性是否还是按照这种方案去找patch引入新特性解决？且这个方法会耗费大量人力和合入大量新特性patch带来未知的风险。

3.4.建议的方案：

 建议优选方案1：

1. 在openEuler20.03 LTS版本引入chromium和gcc 9.3，用户需要安装chromium就必须先装gcc9.3，这不会影响原有软件的兼容性，但是后面新安装的软件必须都要用gcc9.3编译（OS上只能存在一个gcc，如果退回gcc7.3，libstdc++.so等gcc运行库也会回退，导致chromium无法运行）。gcc7.3和chromium无法并存。
2. 其他业界OSV社区，不会在LTS版本上升级软件大版本，软件大版本的升级会引入新特性、ABI兼容性等风险，且OS涉及上千个外围包，如果都要升级，会导致LTS版本面目全非，影响版本稳定性。软件大版本的升级一般都是用户自己下载安装。业界社区也不会在LTS版本上引入新软件来替换老的软件，这会导致已有用户被迫使用新软件。
3. 在gcc7.3上打patch的方式来引入新c++特性来支持chromium编译，质量风险较大，社区gcc引入新特性后会有长达半年以上的维护周期，期间会合入大量bugfix，比如gcc7的特性开发完毕到gcc7.3发布长达8个月，涉及bugfix数量2500+个。该方案在开发阶段较为合理，在维护阶段不太合适。