**终端 E5170s-22TCPU-V200R001B200D01SP05C00**

**开源软件认证报告**

**第一部分：综述**

1. **自研代码风险分布**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 开源软件使用情况 | 类别 | 风险 | 规避方式 | 综述 |
| 确定使用的开源软件 | 开源风险 | 低 | NA | 无对外开源风险；  严重开源软件安全漏洞 |
| 开源软件安全  漏洞 | 严重 | 无 |
| 疑似使用的开源软件 | 开源风险和漏洞 | NA | NA |

1. **非自研文件列表**

|  |  |
| --- | --- |
| 非自研文件类别 | 名称 |
| 公司内部平台 | 海思Balong V700R001C35B200 |
| 供应商 | Broadcom、Realtek |

**结论：送检版本自研代码使用了高风险开源软件，根据法务的意见，在产品描述的使用场景下，产品代码不存在对外开源的风险；开源软件存在严重风险安全漏洞。产品的开源风险和安全漏洞还取决于平台和供应商。**

具体使用方式为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 软件 | 使用申请单编号 | 许可证 | 使用场景 | 使用方式 | 应用IPR风险 |
| 软件1 | 00986817  第2个软件 | [GPL V2.0](http://pdm.huawei.com/Windchill/navigator/html/ext/huawei/opensource/license/licenseview.html?oid=VR:ext.huawei.huaweipart.HuaweiPart:3762365940) | 集成到华为产品 | 通过fork或exec或script调用 | 低 |
| 软件2 | 00986817  第7个软件 | LGPL V2.1 | 集成到华为产品 | 动态链接 | 低 |
| 软件3 | 00986817  第8个软件 | [GPL V2.0](http://pdm.huawei.com/Windchill/navigator/html/ext/huawei/opensource/license/licenseview.html?oid=VR:ext.huawei.huaweipart.HuaweiPart:3762365940) | 集成到华为产品 | 通过fork或exec或script调用 | 低 |
| 软件4 | 00986817  第9个软件 | LGPL V2.1 | 集成到华为产品 | 通过fork或exec或script调用 | 低 |
| 软件5 | 00986817  第12个软件 | [GPL V2.0](http://pdm.huawei.com/Windchill/navigator/html/ext/huawei/opensource/license/licenseview.html?oid=VR:ext.huawei.huaweipart.HuaweiPart:3762365940) | 集成到华为产品 | 通过fork或exec或script调用 | 低 |

**第二部分：认证概述**

**一、认证结果概述**

1. 送检版本确定使用13个开源软件，其中包含3个GPL开源软件，2个LGPL开源软件，所有软件都已提交开源软件申请电子流，电子流评审通过，经IPR评审风险等级最高为：低。
2. 送检版本存在平台文件，其大小占总量59.69%，未对该部分文件进行认证。
3. 送检版本存在供应商提供的文件，其大小占总量2.10%，未对该部分文件进行认证。
4. 送检版本所使用的开源软件存在3个安全漏洞。

**【产品澄清的邮件】**



**二、风险概述**

1. 送检版本所使用的开源软件存在安全漏洞，可能会导致系统不正常工作或者黑客攻击，大T/国家安全认证不通过。
2. 送检版本存在供应商提供的文件，风险未知。

**三、下一步的建议**

1. 对于所使用的开源软件，需按照License规定正确使用、履行对外声明义务。
2. 对于平台文件的开源风险，请向相关业务部门申请平台开源软件认证报告。
3. 对于来自供应商的文件，应通过开源软件协议来排除风险，在该项目的下一个DCP点给出处理方案。
4. 产品送检时声明为内部使用的文件,因其不对外发布,可认为无开源风险。如果后续此部分文件要对外发布，需重新进行开源认证。
5. 送检版本使用的开源软件有3个安全漏洞，开源软件安全漏洞由于漏洞信息公开，可能会导致恶意攻击，并进而影响业务正常运行或信息泄漏，因此产品需要针对高、中风险的开源安全漏洞给出修复方案或规避措施，必要时寻求各产品线安全工程部进行方案支撑。

**第三部分：详细报告**

1. **送检版本文件分布**

Etrans单号: 900136148BBBBBBB47767A8325ADCD35，文件大小2 G，文件数 26092 Files。

送检版本PDM认证电子流单号：00968122

项目在SVN配置库中路径及对应的标签为：

|  |  |
| --- | --- |
| 库路径 | 对应的标签 |
| http://siasvn02-rd:6801/svn/TC\_LTE\_balongV7R1\_SVN/V700R001C35B200/branches/BR\_E5170s-22 | 13444 |

送检版本详细的文件清单已在检测中心备案。

|  |  |
| --- | --- |
| 来源类型 | 代码比例 |
| 确定的开源软件代码 | 0.98% |
| 自研代码 | 5.69% |
| 内部使用代码 | 31.54% |
| 平台文件 | 59.69% |
| 供应商文件 | 2.10% |

1. **送检版本确认使用的开源软件**

|  |  |
| --- | --- |
| 许可证类型 | 开源软件个数 |
| GPL 2.0 | 3 |
| LGPL 2.1 | 2 |
| Apache License Version 2.0 | 1 |
| BSD 2.0 | 4 |
| Curl License | 1 |
| MIT License V2 | 1 |
| zlib/libpng License | 1 |
| 总计 | 13 |

建议：

1. GPL类型的开源软件具有传染性，若以导致开源的方式使用了GPL类型的开源软件，处理方式可参考：
   1. 履行开源义务：代码开源或提供Written offer给出代码获取方法。
   2. 版本受限销售：经相关业务决策机构批准，版本受限销售且给出软件替换计划和风险发生后处理方法。
   3. 移除开源软件：将可能导致产品开源的软件移除，替换为其他无开源风险的软件或自研。
2. LGPL开源软件在动态链接的情况下不需要开源，除非是以动态链接的方式使用，否则请参考GPL类型开源软件处理方式。
3. 对于所使用的开源软件，需按照License规定（含例外声明）正确使用。
4. **送检版本疑似使用的开源软件**

无

1. **送检版本使用的平台文件**

认证的代码中包含平台文件，平台代码由平台部门单独进行认证。

建议：平台代码的开源软件认证报告请向相关业务部门申请。

1. **送检版本使用了供应商提供的文件**

建议：对于来自供应商的文件，应通过开源软件协议来排除风险，在该项目的下一个DCP点给出处理方案。

1. **送检版本所使用开源软件的安全漏洞情况**

送检版本所使用的开源软件存在3个安全漏洞。

|  |  |
| --- | --- |
| 漏洞严重程度 | 漏洞个数 |
| 高 | 1 |
| 中 | 2 |
| 低 | 0 |
| 总计 | 3 |

建议：

开源软件安全漏洞由于漏洞信息公开，可能会导致恶意攻击，并进而影响业务正常运行或信息泄漏，因此产品需要针对高、中风险的开源安全漏洞给出修复方案或规避措施，必要时寻求各产品线安全工程部进行方案支撑。

开源软件认证中心

2013年07月08日