**文档密级：**公司内部A

**AI研究院**

**引擎编译安全管理规定**

制作人：张国红

审批人：工程委员会

发布日期：2020年10月26号

版本记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 版本号 | 更改时间 | 更改内容描述 | 填写人 |
| 1 | V1.0 | 2020/10/26 | 新建 | 张国红 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[一、 目的与原则 5](#_Toc54339283)

[1.1 目的 5](#_Toc54339284)

[1.2 原则 5](#_Toc54339285)

[二、 术语定义 5](#_Toc54339286)

[三、 管理组织与职责 5](#_Toc54339287)

[3.1 工程委员会 5](#_Toc54339288)

[3.2 内核技术部 5](#_Toc54339289)

[3.3 引擎研发负责人 5](#_Toc54339290)

[3.4 引擎测试负责人 5](#_Toc54339291)

[3.5 QA 5](#_Toc54339292)

[四、 引擎编译要求 6](#_Toc54339293)

[4.1 安全编译选项列表 6](#_Toc54339294)

[五、 验证方法 7](#_Toc54339295)

[六、 相关文件及执行模板 7](#_Toc54339296)

[5.1 参考链接 7](#_Toc54339297)

[5.2 参考样例 7](#_Toc54339298)

[七、 备注说明 7](#_Toc54339299)

# 目的与原则

## 目的

规范引擎安全编译方法，保障RDG引擎运行安全，防止引擎被外部破解。

## 原则

该规定适用所有RDG发布的内核引擎， 并纳入底线审计作为对引擎发布的基本要求。

# 术语定义

无

# 管理组织与职责

## 工程委员会

规范要求及执行方法的审核；

## 内核技术部

引擎安全编译前期的技术验证

## 内核质量部

安全编译选项检测工具的开发、验证

## 引擎研发负责人

对待发布的引擎进行安全编译

## 引擎测试负责人

对引擎安全编译的执行结果进行验证，并在测试报告中有明确的结论

## QA

对各引擎产品执行的结果进行审计，并反馈审计结果

# 引擎编译要求

RDG所有发布的引擎都需要在编译时添加《安全编译选项列表》中指定的选项

## 安全编译选项列表

|  |  |  |  |
| --- | --- | --- | --- |
| **安全编译选项** | **描述** | **编译参数** | **编译工具** |
| BIND\_NOW | 立即绑定 | -Wl,-z,now | gcc |
| NX | 堆栈不可执行 | -Wl,-z,noexecstack | gcc |
| PIC | 地址无关 | -fpic -shared | gcc |
| PIE | 随机化 | -fpie -Wl,-pie | gcc |
| RELRO | GOT表保护 | -Wl,-z, relro | gcc |
| SP | 栈保护 | -fstack-protector –fstack-protector-all | gcc |
| NO Rpath/Runpath | 动态库搜索路径（禁选） | -Wl,--disable-new-dtags,--rpath [path] | gcc |
| FS | Fortify Source | –D\_FORTIFY\_SOURCE=2 | gcc |
| Ftrapv | 整数溢出检查，该选项可能带来性能损失，暂不做强制要求 | -ftrapv | gcc |
| Strip | 符号表删除 |  | gcc-strip |
| Bsymbolic | 优先使用本地符号表 | -Wl,-Bsymbolic | gcc |
| FormatCheck | 字符串格式安全检查 | -Wformat = 2 -Wformat-security | gcc |
| fvisibility | 动态库符号隐藏 | -fvisibility=hidden | gcc |

# 验证方法

使用OptionCheckTool工具对引擎so进行验证，输出结果中除Trapv外其它所有参数标绿时即为通过。

# 相关文件及执行模板

## 参考链接

https://developers.redhat.com/blog/2018/03/21/compiler-and-linker-flags-gcc/

https://www.owasp.org/index.php/C-Based\_Toolchain\_Hardening

## 参考样例

makefile安全编译参数参考样例

CFLAGS =“-Wall -Wextra -Wconversion -fPIE -Wno-unused-parameter

-Wformat = 2 -Wformat-security -fstack-protector-all -Wstrict-overflow”

LDFLAGS =“-pie -z，noexecstack -z，noexecheap -z，relro -z，now -Wl,-Bsymbolic”

# 备注说明

以上编译选项在Maxengine-Android-armv8和Maxengine-armlinux-armv8 上进行测试，测试发现存在编译器版本差异，当不支持时请删除；编译器选项在CFLAGS\LDFLAGS中均添加即可，编译器将自动识别。

* 使用Strip选项后，现场问题如何调式：

可参见：[http://wiki.iflytek.com/pages/viewpage.action?pageId=303944546](http://wiki.iflytek.com/pages/viewpage.action?pageId=303944546" \t "_blank)

或参见文档《strip的so调试方法.doc》

* 引擎安全编译问题接口人：内核技术部 李必然（brli）
* 检测工具问题接口人：内核质量部 潘松（songpan）