



HiSparkStudio 版本描述文件

文档版本 01

发布日期 2024-07-16

版权所有 © 海思技术有限公司2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HISILICON、海思和其他海思商标均为海思技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

海思技术有限公司

地址：上海市青浦区虹桥港路2号101室 邮编：201721

网址：<https://www.hisilicon.com/cn/>

客户服务邮箱：support@hisilicon.com



前言

概述

本文档主要介绍IDE的版本信息。






读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 软件开发工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
 警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
 注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
 须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
 说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。



修改记录

修订日期	版本	修订说明
2023-06-30	00B01	第1次临时版本发布。
2024-02-21	00B02	第2次临时版本发布。 1.0.0.1版本说明。 刷新版本更新文档说明。
2024-03-15	00B03	第3次临时版本发布。 删除1.0.0.1版本说明，新增1.0.0.2版本说明。
2024-07-16	01	第1次正式版本发布。 删除1.0.0.2版本说明，新增1.0.0.7版本说明。 新增5 对前一基础版本不足之处的改进。 新增版本遗留问题。



目 录

前 言..... i

1 版本基本信息..... 1

2 版本限制说明..... 2

3 版本配套信息表..... 3

4 安装和升级使用说明..... 4

5 对前一基础版本不足之处的改进..... 5

6 对前一基础版本新增、修改和删除的功能特性..... 6

 6.1 新增的功能特性..... 6

 6.2 修改的功能特性..... 6

 6.3 删除的功能特性..... 7

7 开源及第三方软件漏洞修复列表..... 8

8 版本遗留问题..... 12

9 版本硬件变更说明..... 13

10 版本更新文档说明..... 14



1 版本基本信息

产品名称	HiSpark-Studio	
版本号	1.0.0.7	
版本适用MCU	支持3065HRPIRZ、3065HRPICZ、3061HRPIKZ、3065ARPIRZ、3061MNPICA、3061MNPIKA、3061MNNIKA、3061MNNICA、3061MNPIC8、3061MNPIC8、3061MNNIK8、3061MNNIC8	
版本类型	√	基础版本
	不涉及	累积补丁
	不涉及	紧急补丁
版本发布原因	修复遗留问题。	



2 版本限制说明

使用限制	时 间 限 制	截至下个版本发布。
	发 布 范 围	受限。
	是否可商用	商用。
	其他限制条件	仅用于客户软硬件联调。
	版本终止条件	下个版本发布。



3 版本配套信息表

序号	插件名称	插件版本号
1	hisparkbase.vsix	0.0.1
2	hisparkburntool.vsix	0.0.7
3	hisparkcompile.vsix	0.0.1
4	cpptools-win32.vsix	1.19.2
5	hisparkchipconfig.vsix	0.0.1
6	hisparkdevicetooldebug.vsix	0.0.1
7	hisparkfileicontheme.vsix	1.0.0
8	khisparkvscodekeyboardshortcuts.vsix	0.0.1
9	hisparkprogress.vsix	0.0.1
10	hisparkprojectwizard.vsix	0.0.4
11	hisparkprojectanalysis.vsix	0.0.1
12	hisparkstatusbarmodify.vsix	0.0.1
13	hisparktoolbardefault.vsix	0.0.1
14	hisparkwelcomepage.vsix	0.0.1
15	MS-CEINTL.vscode-language-pack-zh-hans.vsix	1.68.3
16	hisparkiarkeyboardshortcuts.vsix	0.0.1
17	hisparkkeilkeyboardshortcuts.vsix	0.0.1



4 安装和升级使用说明

请参考《HiSparkStudio 使用指南》。



5 对前一基础版本不足之处的改进

在工具运行的过程中，遇到文件没有读写权限、文件不存在、文件被篡改等情况时，系统将给出明确的错误提示。这些提示信息将详细说明出现错误的原因，并提供可能的解决方案。。



6 对前一基础版本新增、修改和删除的功能特性

6.1 新增的功能特性

序号	简要描述	详细描述	修改的模块
1	新增芯片 3065ARPIRZ 、 3061MNNIK A、 3061MNNIC A、 3061MNPIK8 、 3061MNPIC8 、 3061MNNIK8 、 3061MNNIC8	支持对新芯片的创建、编译、调试、烧录和配置功能。	IDE

6.2 修改的功能特性

序号	简要描述	详细描述	修改的模块
1	新增可靠性提示	在工具运行的过程中，遇到文件没有读写权限、文件不存在、文件被篡改等情况时，系统将给出明确的错误提示。这些提示信息将详细说明出现错误的原因，并提供可能的解决方案。	IDE、Programmer



6.3 删除的功能特性

无。



7 开源及第三方软件漏洞修复列表

漏洞信息可通过CVE编号在NVD（National Vulnerability Database）网站查询：
<http://web.nvd.nist.gov/view/vuln/search>。

软件名称	软件版本	CVE编号	漏洞描述	解决方案
electron	18.3.9	CVE-2023-44402	影响启用了“EmbeddedAsarIntegrityValidation”和“onlyLoadAppFromAsar”熔断的应用。未启用这些保险丝的应用不受影响。此问题特定于macOS，因为这些保险丝目前仅在macOS上受支持。	将electron版本升级至22.3.26。
libjpeg-turbo	2.1.2	CVE-2023-2804	基于堆的缓冲区溢出问题。该漏洞只能在12位数据精度下被利用，对于该精度，样本数据类型的范围超出了有效样本范围，因此，攻击者可以手工创建包含超出范围的12位样本的12位无损JPEG图像。	libjpeg-turbo为electron依赖，将electron版本升级为22.3.26解决。



软件名称	软件版本	CVE编号	漏洞描述	解决方案
next.js	12.2.0	CVE-2022-36046	Next.js是一个React框架，可以提供构建模块来创建Web应用程序。必须满足以下所有条件才会受到此CVE的影响： Next.js版本12.2.3, Node.js版本高于v15.0.0, 正在使用严格的'unhandledRejection'退出，并使用next start。	进度条插件和工具栏插件中source-map依赖升级至0.7.4、i18next升级至23.4.6, react升级至18.2.0。
next.js	12.2.0	CVE-2023-46298	Next.js 13.4.20-canary.13之前的版本缺少cache-control头，因此空的预取响应有时可能会被CDN缓存，从而导致通过该CDN请求相同URL的所有用户拒绝服务。	进度条插件和工具栏插件中source-map依赖升级至0.7.4、i18next升级至23.4.6, react升级至18.2.0。
retdec	3.3	CVE-2022-23907	在ir_modifications.cpp的函数canSplitFunctionOn()中，由于堆缓冲区溢出，可能存在越界读取。影响是：拒绝服务、内存泄漏和可能的代码执行。	Cpptools插件引入，插件升级至1.19.2解决。
sqlite	3.37.2	CVE-2022-35737	SQLite 1.0.12到3.39.2之前的3.39.x版本，如果在C API的字符串参数中使用数十亿字节，有时会允许数组边界溢出。	Cpptools插件引入，插件升级至1.19.2解决。



软件名称	软件版本	CVE编号	漏洞描述	解决方案
sqlite	3.37.2	CVE-2022-46908	SQLite到3.40.0，当依赖--safe执行不受信任的CLI脚本时，不会正确实现azProhibitedFunctions保护机制，而是允许使用诸如Writefile之类的UDF函数。	Cpptools插件引入，插件升级至1.19.2解决。
sqlite	3.37.2	CVE-2023-7104	此问题影响组件make alltest Handler的文件ext/session/sqlite3session.c中的函数sessionReadRecord。该操作会导致基于堆的缓冲区溢出。	Cpptools插件引入，插件升级至1.19.2解决。
zlib	1.2.11	CVE-2022-37434	在inflate.c中通过一个大的gzip标头额外字段在inflate中具有基于堆的缓冲区过度读取或缓冲区溢出。	qt5.15.8引入，通过打补丁解决。
zlib	1.2.11	CVE-2023-45853	MiniZip在zlib 1.3版本及之前的版本中存在一个整数溢出漏洞和由此引起的堆缓冲区溢出漏洞，漏洞出现在zipOpenNewFileInZip4_64函数中，攻击者可以通过一个较长的文件名、注释或额外字段来利用该漏洞。	qt5.15.8引入，通过打补丁解决。
zlib	1.2.11	CVE-2018-25032	如果输入有许多远程匹配，zlib会出现在压缩时内存损坏。	qt5.15.8引入，通过打补丁解决。



软件名称	软件版本	CVE编号	漏洞描述	解决方案
pcre2	10.39	CVE-2022-1586	攻击者利用该漏洞通过 pcre2_jit_compile.c 中的 compile_xclass_matchingpath 强制读取 PCRE 的无效内存地址，以触发拒绝服务或获取敏感信息。	qt5.15.8引入，通过打补丁解决。
pcre2	10.39	CVE-2022-1587	攻击者利用该漏洞通过 pcre2_jit_compile.c 中的 get_recurse_data_length 强制读取 PCRE 的无效内存地址，以触发拒绝服务或获取敏感信息。	qt5.15.8引入，通过打补丁解决。



8 版本遗留问题

序号	问题描述	级别	问题影响	规避措施
1	低概率：HiIDE使用时cpptools挂掉，注释的变色功能失效、静态代码规范不检查。	一般	代码静态检查功能失效。	重启IDE之后功能恢复正常。
2	调试时，将反汇编代码和源代码同时打开执行调试，反汇编代码和源代码有时不可同步跟随。	一般	在跟随汇编代码时，当进入到非汇编代码之后，跳出来时不会自动回到汇编界面。	手动点击汇编页面，进入到汇编页面之后，可以继续跟随。
3	工程调试中的监视窗口，当展开一个数据量超过3000的变量时，调试无法正常使用。	一般	调试功能需要等待很长时间。	避免一次监视超过3000个子项的复杂变量，可以采用直接监视复杂数据结构中的某些简单的子项的方式来规避。
4	在汇编文件中打断点，会超过断点允许的上限。	一般	导致调试异常，自动退出	删除一些断点之后，再次启动调试。306x系列允许7个断点，3061M系统允许3个断点。



9 版本硬件变更说明

本章节描述硬件相对上一个版本的重要变更以及对底层软件的影响。

序号	问题描述	涉及模块	注意事项
1	无	-	-



10 版本更新文档说明

请参见版本交付件清单。

文档名称	文档版本号	文档更新说明
Programmer 使用指南	01	第1次正式版本发布。 刷新第2章节界面说明、第4章节烧写说明。 更新图片。
Motor Control Workbench 使用指南	01	第1次正式版本发布。 删除3.4章节表达冗余的部分。 修改第2、3、4章节的图片。
HiSpark调试器系列 使用指南	01	第1次正式版本发布。 更新4.2章节和5.1章节图片。
VariableTrace 使用指南	01	第1次正式版本发布。 删除第5章，参数说明冗余表达的部分。 更新2、3、4章节的图片。
工具软件 二次开发网络安全注意事项	01	第1次正式版本发布。 修改了发布的工具名字，从Flasher改成Programmer