工具软件 二次开发网络安全注意事项

文档版本　00B01

发布日期　2023-06-01

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

本文旨在从网络安全的角度，介绍工具软件使用过程中的网络安全注意事项，帮助客户消除网络安全风险。本文提到工具软件属于SolarA^{2}解决方案的配套工具。

读者对象

本文档（本指南）的读者为开发工程师。

修订记录

修订日期	版本	修订说明
2023-06-01	00B01	第1次临时版本发布。

目 录

插图目录

表格目录

1 概述

本文提到的工具软件属于SolarA2解决方案SDK的配套工具，客户可基于SolarA2解决方案SDK进行业务二次开发，按需开发出自定义的各种形态的产品。提供工具软件的目的是支撑客户高效便捷的开展二次开发及调测工作。在二次开发调测过程中，工具软件需要与产品MCU进行通信，因此需要MCU提供相应配合。但在二次开发完成后，产品发给最终消费者前，需从网络安全的角度调整MCU配置。软件工具不需要也不允许发布给产品的最终消费者。

1.1 版本交付内容说明

基础版本基于Java 和 C++开发。版本交付的工具产品如表1-1所示。

表 1-1 版本交付的工具产品

工具名	工具类别	备注
Flasher	UART/JTAG/SWD口烧写工具	针对嵌入式系统提供镜像烧录功能
variabletrace	JTAG/SWD口调试工具	针对嵌入式系统提供变量监控功能

2 工具软件网络安全分析

2.1 安全攻击及威胁

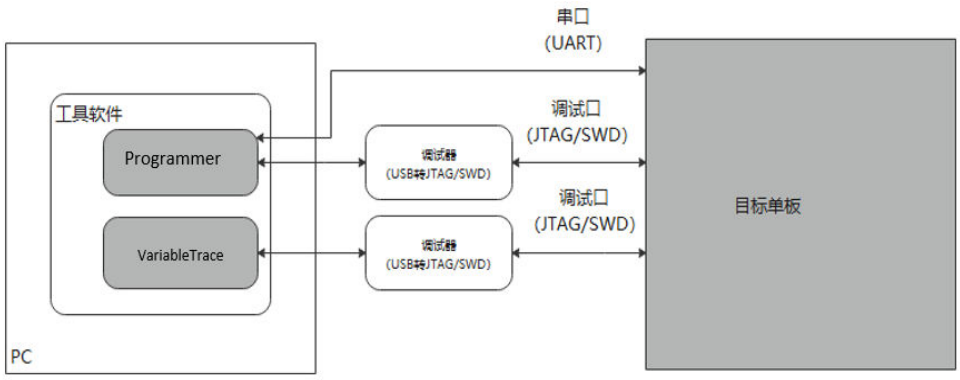
工具软件均为PC上运行的单机软件，需要通过硬件接口与目标单板进行通信，主要涉及的接口如表2-1所示。

表 2-1 工具与通信方式

工具	通信方式
Programmer	USB口转JTAG/SWD口或者串口
VariableTrace	USB口转JTAG/SWD口

工具软件的组网结构如图2-1所示。

图 2-1 工具软件使用组网



如图2-1所示，目标单板通过调试接口（JTAG/SWD口）或串口与电脑相连。

Programmer通过调试端口或串口可以对目标单板进行烧录镜像和读取镜像。这些可能成为黑客对设备攻击的手段。

variabletrace通过调试端口可以对目标单板进行调试。调试包括查看和修改运行时的变量值。这些可能成为黑客对设备的硬件、软件、配置参数进行分析的重要手段。

2.2 安全面

2.2.1 管理

工具软件仅供在产品开发过程使用，不随产品发布给最终消费者。工具软件在使用时需配置目标单板MCU型号信息，作为与目标单板建立通信和选择烧录算法的依据。

2.2.2 控制

工具软件在运行时仅作为数据传输通道，不存储和控制在烧录、调试过程中的数据，不涉及敏感信息处理。

工具软件Programmer在使用调试器时硬件通过JTAG/SWD口与目标单板连接，也可以通过串口直接连接电脑。运行时先将目标单板的烧录程序传输到目标单板并运行，再将镜像文件传输到目标单板，由烧录程序将镜像文件写入目标单板MCU的Flash上。基于烧录程序，工具软件还支持复位目标单板和读取目标单板MCU Flash上的镜像文件。

工具软件variabletrace在使用调试器硬件通过JTAG/SWD口与目标单板连接时，工具软件先与目标单板建立调试连接，再对目标板程序进行调试，查看变量地址所存储的数据。

2.2.3 使用

工具软件不涉及联网、不涉及用户隐私数据。

2.3 其他使用安全注意事项

2.3.1 PC 调试工具

- 工具软件Flasher运行在PC上，对目标单板进行镜像文件烧录、镜像文件读取和复位操作。
- 工具软件variabletrace运行在PC上，对目标单板的指定内存地址读取或者写入数据。

2.3.2 调试接口

工具软件工作时，需目标单板允许研发过程保留调试端口用于调试，但正式发货的目标单板建议关闭调试端口（JTAG/SWD口）和串口，防止目标单板内的信息泄露。

工具软件Flasher 需目标单板开启调试串口，建议客户在安全敏感的发货产品上采取以下措施：

1. 将串口从目标单板物理上删除；
2. 禁止串口、禁止串口升级功能，禁止方法请参见《Hi306xH系列技术参考指南》。

工具软件Flasher和variabletrace需目标单板开启JTAG/SWD口，建议客户在安全敏感的发货产品上采取以下措施：

1. 将JTAG/SWD口从目标单板物理上删除；
2. 禁止JTAG/SWD口功能，禁止方法请参见《 Hi306xH系列技术参考指南 》。

2.3.3 镜像安全

工具软件不携带烧录、调试用的镜像文件，镜像文件由用户提供，例如通过IDE工具编译用户的工程代码生成镜像文件。

3 结论

综合以上章节，总结网络安全如下：

- 工具软件属于开发调测工具，仅供开发过程中使用，不能发给最终消费者；
- 工具软件不涉及联网、不涉及用户隐私数据，仅通过调试端口访问目标单板；
- 工具软件需要使用目标单板调试端口，但正式发货的目标单板建议关闭调试端口（JTAG/SWD口）和串口，防止目标单板内的信息泄露。