WS73V100 二次开发网络安全

注意事项

文档版本　02

发布日期　2024-10-21

深圳市安信可科技有限公司

前言

概述

WS73V100 交付包为芯片解决方案交付包，主要包括芯片资料、硬件资料、SDK 软件包、软件参考设计以及软件资料等。用户可基于此芯片解决方案交付包，开发各种自定义的产品。

本文档从网络安全的角度，重点分析基于本交付包开发的产品在使用过程中，可能面临的与本交付包中 SDK 软件包相关的网络安全的威胁，同时，针对性地给出相应的解决方案。

产品版本

与本文档相对应的产品版本如下。

产品名称	产品版本
WS73	V100

读者对象

本文档主要适用于以下工程师：

- 技术支持工程师
- 软件开发工程师

深圳市安信可科技有限公司

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

文档版本	发布日期	修改说明
02	2024-10-21	新增“1.1 免责声明”章节内容。
01	2024-08-09	第一次正式版本发布。

深圳市安信可科技有限公司

目 录

前言 i

1 产品安全解决方案 1

1.1 免责声明 1

1.2 安全架构 1

1.3 设备安全 2

1.4 硬件设计安全注意事项 2

1.4.1 串口 2

1.4.2 JTAG 调试 2

1.5 其他使用安全注意事项 3

1.5.1 JTAG 接口 3

1.5.2 代码安全注意事项 3

1.5.3 可维可测注意事项 3

2 结论 5

深圳市安信可科技有限公司

1 产品安全解决方案

1.1 免责声明
1.2 安全架构
1.3 设备安全
1.4 硬件设计安全注意事项
1.5 其他使用安全注意事项

1.1 免责声明

客户应充分评估自身产品的网络安全要求（包括但不限于：在实际量产产品中，选择安全加解密算法、关闭不安全协议 telnet、关闭不需要的调试接口和命令等），并承担最终责任。本产品提供的本注意事项文档帮助客户对自身产品进行网络安全加固。

本产品在本文档中所描述的部分功能使用到了密钥来提供安全机制，客户需要妥善生成、烧写、使用并管理密钥（包括但不限于非对称密钥、对称密钥等），否则将自行承担相关风险。

1.2 安全架构

产品的网络安全是一个系统工程，涉及到整个产品的各个层面。

WS73 版本可能涉及的威胁包括：

- JTAG 安全调试

  JTAG 调试功能默认开启，建议产品量产时关闭 JTAG 调试功能。

深圳市汉信可科技有限公司

1.3 设备安全

基于安全性考虑，建议用户在最终产品中执行以下措施：

- 永久关闭 JTAG 调试功能，关闭方法参照“1.4.2 JTAG 调试”和“1.5.1 JTAG 接口”。
- 关闭 DebugKits 调试工具，关闭方法参照“1.5.3 可维可测注意事项”

1.4 硬件设计安全注意事项

1.4.1 串口

UART0 的安全防护设计有以下两种方案，根据产品的安全需求选择合适的方案：

- 设备出厂前去除 UART0 信号选焊电阻，确保 UART0 信号断链；

  去掉连接器（或排针）、在 PCB 上删除连接器和 UART0 信号的丝印，UART0 信号不走 PCB 表层。在远离 UART0 插座的位置，在 TX，RX 信号上增加选焊电阻，发货前至少去除选焊电阻。
- 直接去掉 UART0 信号链路。

1.4.2 JTAG 调试

JTAG 的安全防护设计有以下两种方案，根据产品的安全需求选择合适的方案：

- 设备出厂前去除 JTAG 信号选焊电阻，确保 JTAG 链断链；

  去掉连接器（或排针）、在 PCB 上删除连接器和 JTAG 信号的丝印，JTAG 信号不走 PCB 表层。在远离 JTAG 插座的位置处，在 TCK、TDI、TDO 信号上增加选焊电阻，发货前至少去除其中一个选焊电阻，同时打乱 JTAG 焊点分布（指用于焊接 JTAG 连接器关键信号引脚的焊点在 PCB 布局中“打乱”，与其它功能焊点进行混淆）。
- 直接去掉 JTAG 信号链路。

深圳市安信可科技有限公司

1.5 其他使用安全注意事项

1.5.1 JTAG 接口

JTAG 调试功能是研发阶段常用的一种调试手段，能够进行单步调试，查看或修改寄存器、变量的值，攻击者可以通过该接口对系统发起攻击。WS73 芯片 JTAG 调试功能默认开启，主要用于客户二次开发时进行调试。产品上市时必须关闭 JTAG 调试功能。可以在产品产测阶段通过烧写 EFUSE 关闭 JTAG 调试功能。具体命令如下：

```
echo "wlan0 set_jtag_disable 1" > /sys/ccsys/ccpriv   #参数传1表示关闭JTAG调试功能
echo "wlan0 get_jtag_disable " > /sys/ccsys/ccpriv   #查询JTAG调试功能是否关闭
```

须知

注意 EFUSE 只能写一次，写完后就无法修改。

1.5.2 代码安全注意事项

代码错误引发的网络安全问题，一般都是源于最基本的代码规范问题，例如：指针越界、数组越界、入参不检查等错误。建议通过如下方法检查：

- 使用业界通用的代码健康扫描工具进行全覆盖扫描。
- 使用模糊测试工具，对所有 API 接口（包括设备驱动接口）进行全范围模糊测试。
- 使用业界通用的漏洞扫描工具对所使用的开源软件进行扫描。

1.5.3 可维可测注意事项

SDK 包提供如下调试组件：DebugKits：用于 WS73 SDK 日志输出和调控。
DebugKits 具有以下性质：

- DebugKits 是 WS73 调试工具，通过 DebugKits 工具可以查看到 SDK 输出的各种日志信息，并可通过工具界面对 WS73 发起操控；
- DebugKits 工具运行在 Windows PC 上，通过网口或者串口连接到 WS73 对接的主控芯片；
- WS73 SDK 开放 TCP 端口号 30000，用于侦听 DebugKits 工具接入；

该工具不在网调测，不能被用于任何的客户实际的发布产品中，上述工具不具有用户鉴权功能，需要注意工具的信息安全保护，以防外泄对产品造成影响。

深圳市云信可科技有限公司

客户提供的输入数据，需要客户保证得到了授权与许可，且客户承担相应的隐私保护责任义务。工具只对输入数据进行数学运算，不对其内容进行分析。

⚠ 警告

- DebugKits 工具没有安全认证机制，传输通道也不支持安全传输机制，仅用于二次开发过程中调试使用；
- 为避免产品上市后，攻击者利用该端口攻击产品，产品量产时必须关闭 SDK 中的 DebugKits 调试功能，关闭方法如下：

将文件 sdk\linux\build\config\ws73_default.config 中的 WSCFG_PLAT_DIAG_LOG_OUT 宏关闭后再编译发布版本。

```
# WSCFG_PLAT_DIAG_LOG_OUT is not set
```

深圳市安信可科技有限公司

2 结论

WS73 产品有必要基于安全威胁分析采取相对应的安全措施。以下安全原则供参考：

- 适度的安全

  安全设计是基于特定的安全危险场景分析，考虑到性能、成本、业务影响，决策采用最合适的安全措施。

- 最小授权

  根据职责的需要，给用户、维护人员、网络单元、程序、进程等授予最小的权限和资源。这样能减少潜在的安全风险。

- 主动协同防御

  及时识别恶意攻击源，并在攻击造成显著危害前自动删除恶意用户和网络之间的连接。也可以降低连接的带宽和服务质量，以尽量减少负面影响。

- 纵深防御

  纵深防御原则涉及到对威胁的多重防御。例如，当一个防御层不够时，另一个防御层将防止造成进一步破坏。

深圳市安信可科技有限公司