阿里云
IoT固件安全检测

产品简介

文档版本：20200203

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. **您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。**
2. **未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。**
3. **由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。**
4. **本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。**
5. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。**
6. **如若发现本文档存在任何错误，请与阿里云取得直接联系。**

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

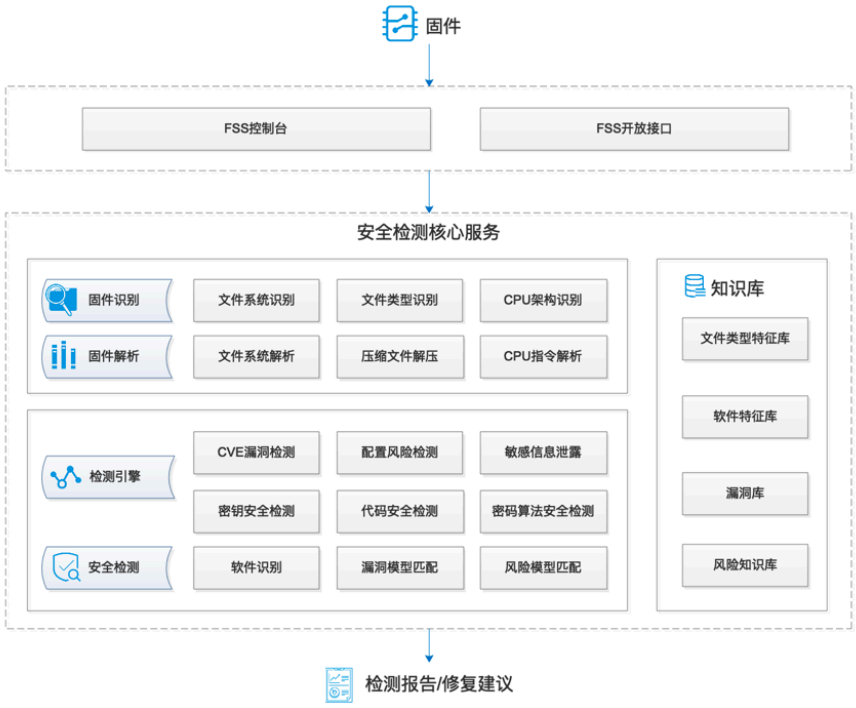
1 什么是IoT固件安全检测

IoT固件安全检测，简称FSS，主要提供IoT设备固件的安全检测服务，检测设备固件的安全风险，如已知软件CVE漏洞，敏感信息等，并提供安全修复建议。

FSS针对IoT设备固件提供无侵入的安全检测服务，提前发现安全风险，提升IoT设备安全强度，降低厂商因固件漏洞导致的更新、回收以及OTA更新升级成本，提升各种IoT设备的基础安全水位。

产品架构

用户提交固件到FSS，FSS自动化进行安全检测，检测完成后生成安全检测报告并发送通知邮件。FSS的架构如下图所示：



FSS由三部分组成：FSS控制台、开放接口、安全检测核心服务。

1）FSS控制台

您可以用阿里云账号登录到FSS控制台，可以在FSS控制台中提交固件进行安全检测、查看检测报告、查看检测报告的分析、管理检测任务等操作。

2）开放接口

您可以使用FSS开放接口的方式进行固件安全检测、检测任务管理等。当前提供的接口包括创建检测任务、查询检测状态、查询检测报告、删除检测任务、查询用户授权信息等。

3）安全检测核心服务

负责固件的安全检测的后台服务，由固件识别、固件解压、检测引擎、知识库等组成。

应用场景

IoT固件安全检测典型应用场景如下：

1）安全开发流程（SDLC）：IoT设备厂商可将FSS嵌入在安全开发流程中，在设备固件发布前上传设备固件，导出安全检测报告，然后根据安全检测报告的建议完成修复、更新设备固件。

2）设备固件升级：IoT设备厂商或OTA厂商上传设备固件升级包，固件检测服务检测并导出安全检测报告，然后根据安全检测报告的建议完成修复、更新设备升级包。

3）固件安全评估：安全检测机构或IT供应链管理人员将固件提交FSS，获取安全检测报告，根据检测结果评估固件的安全风险等级。

说明:
同时FSS支持私有化部署，如果您有私有化部署需求请联系我们

2 功能特性

FSS提供固件的安全检测、检测报告查看等功能。当前检测能力覆盖CVE漏洞、配置风险、密钥安全、敏感信息泄露、代码安全5大类型。

支持2大类固件

支持Linux、RTOS系统固件，包括且不限于Yocto、OpenWrt、uClinux、Android、AliOS Things等。

支持16类安全风险检测

覆盖已知的CVE漏洞、密钥安全、配置风险、信息泄露、代码安全等维度的风险检测。

安全检测能力概览

分类	风险名称\操作系统	类Linux	RTOS(AOS)
CVE漏洞	开源组件CVE漏洞检测	支持	支持
	Linux发行版软件包漏洞	支持	
配置风险	系统弱密码检测	支持	O
	非必要软件检测	支持	
	自启动服务风险检测	支持	
	公开AOS Secret检测		支持
密钥安全	私钥安全检测	支持	支持
	证书安全检测	支持	支持
敏感信息泄露	SVN信息泄露	支持	
	Git信息泄露	支持	
	vi/vim信息泄露	支持	
	备份文件泄露	支持	
	临时文件泄露	支持	
	源代码泄露	支持	
	二进制文件中的信息泄露	支持	支持
	AOS Secret明文存储检测		支持
代码安全	不安全库函数使用检测	支持(上传单个Elf)	支持 (上传单个Elf)

3 产品优势

自动化的云检测引擎

无需源代码、不依赖Agent、二进制文件的黑盒扫描。一步提交、全自动化检测和报告展示。

全面的风险检测

包括漏洞检测、危险评估、弱密码、密钥、敏感数据检测等。

数据资产严格保密

您上传的固件程序、检测报告本身及其内容均采用加密形式存储，同时报告中的敏感数据进行模糊处理。

灵活的使用方式

可以嵌入到安全开发流程中使用、也可以在任何时候验证固件的安全性。

安全专家服务

提供安全专家服务对检测报告进行深度解读，结合业务场景对安全风险进行评级并提供安全风险修复建议和安全防护解决方案。