|  |  |
| --- | --- |
| **产品名称Product name** | **密级Confidentiality level** |
| **BI大数据平台** | **内部公开** |
| **产品版本Product version** | **Total pages共**33**页** |
| BI DSPT 1.0.3.101 |

**BI大数据平台安全性测试策略**

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 | 张中维 | Date  日期 | 2016-04-21 |
| Reviewed by  评审人 | 林啸鸣 | Date  日期 | 2016-04-21 |
| Approved by  批准 |  | Date  日期 | yyyy-mm-dd |



Huawei Technologies Co., Ltd.  
华为技术有限公司

All rights reserved  
版权所有 侵权必究

修订记录

| **日期** | **修订版本** | **CR号** | **修改章节** | **修改描述** | **作者** |
| --- | --- | --- | --- | --- | --- |
| 2016-04-21 | V1.0 |  |  | 初稿输出完成 | 张中维/wx318675 |
| 2016-04-25 | V2.0 |  |  | 更新**威胁建模分析和测试策略章节** | 张中维/wx318675 |
| 2016-04-28 | V3.0 |  |  | 更新MFS组件WEB测试相关 | 张中维/wx318675 |
| 2016-05-06 | V3.0 |  |  | 替换MFS为NFS并更新相应内容 | 张中维/wx318675 |
| 2016-05-13 | V3.0 |  |  | 删除产品人员相关信息 | 张中维/wx318675 |
| 2016-05-19 | V3.0 |  |  | 刷新风险等级相关内容 | 张中维/wx318675 |

目 录

1 概述 5

2 测试规划 5

2.1 项目分析 5

2.2 分层策略 7

2.3 测试计划 7

2.4 自动化策略 7

2.5 测试工具规划 7

3 安全测试策略 9

3.1 总体测试策略 9

3.2 SDV安全测试策略 37

3.3 SIT安全测试策略 39

3.4 SVT安全测试策略 39

4 参考资料清单 39

4.1 安全基线用例集，构建于TMSS服务器 39

4.2 Web安全测试规范\_V1.4.docx 39

**Keywords 关键词**：终端，EMUI，安全红线，测试策略

Abstract 摘要：安全测试策略主要用于指导安全测试方案的输出，测试计划的安排，测试风险的识别等工作，作用如下：

* 手工测试、自动化测试的分工策略，（SDV/SIT/SVT）各阶段的测试策略，安全测试工具（如：Nessus、NGS）的资源规划，以及明确工具使用配置/规则或策略；
* 产品历史版本或同类产品的安全问题进行继承性分析，明确产品的基线/增量测试策略；
* 针对现网安全问题用例集进行产品针对性梳理，输出测试范围和重点；
* 识别高风险模块，进行针对性的测试分析，提高测试覆盖范围。

**缩略语清单：**

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| ICSL | Internal Cyber Security Lab | 内部网络安全实验室 |
| EMUI | Emotion User Interface |  |
|  |  |  |
|  |  |  |

# 概述

BI大数据平台系统覆盖了数据推送、数据入库、执行网关、批处理计算以及文件服务器等子模块。数据推送工具和数据入库工具使用开源的Talend开发。文件服务器使用操作系统自带的网络共享文件系统NFS。批处理组件使用公司内部已经通过安全红线测试的FusionInsight产品。外部的业务服务器周期性的把产生的日志文件以及数据库数据等推送到本系统，在本系统内部对数据进行清洗、转换、入库、计算以及结果输出等操作通过外部的任务调度系统进行周期性的调度执行，计算结果通过定时任务推送到报表、画像等数据开发人员处。本次测试目的是为了覆盖整个平台系统，基于最新的网络安全红线2.0，排查安全问题，并进行整改。

# 测试规划

## 项目分析

本次测试的输入是BI大数据平台系统BI DSPT 1.0.3.101版本。

测试目标：产品满足公司及终端产品线安全红线要求和消费者BG隐私规范要求。

测试范围：针对安全红线中涉及到的安全扫描工具以及相关要求进行测试，涉及的范围有操作系统安全，协议与接口防攻击，产品开发、发布和安装安全，组网及数据库安全，WEB安全，敏感数据保护，系统管理和维护安全，安全资料，日志及口令安全，监听接口及防止非法监听，消费者BG隐私规范，FUZZ测试等。

**下面是系统组网图：**



**测试模块：**

产品主要部件/模块为大数据平台各组件：TCC、执行网关、FusionInsight、DataPush、DataLoad以及NFS（网络共享文件系统）。

Datapush：主要作用是将云服务业务服务器的文件（日志、搜集的文件），数据（数据库里的）从业务服务器传到BI的文件服务器中。

Dataload：主要作用是将传到BI文件服务器中的文件加载到Hadoop系统中 。

TCC ：Task Control Center，部门自研的任务调度和控制系统，开发人员通过web页面配置任务的类型、执行周期等，TCC通过执行配置再网关机上的脚本执行各类任务。

FusionInsight：批处理计算的主体，包含了HDFS、Hive等大数据处理组件，计算入库的数据，并把输出结果移动到数据通道。

执行网关：TCC通过执行存储在执行网关上的脚本，向数据通道、FusionInsight提交数据推送或者计算任务。**测试维度：**

* A1类：合法监听接口、隐私保护、未公开接口
* A2类：访问通道控制、软件完整性保护、敏感数据与加密保护、日志审计

B类：操作系统加固与防病毒、Web安全、产品开发、发布和安装安全、数据库加固、口令安全、敏感数据保护、访问通道控制

**测试重点：**

* 敏感信息/数据存储和传输；
* 协议与接口防攻击；
* WEB安全
* 第三方软件安全性测试以及工具(例如FUZZ等)扫描；
* 组网安全

目前平台系统TCC使用国内环境软件，FusionInsight已过公司安全红线，本次安全测试重点测试执行网关、文件服务器以及数据入库相关组件，对各组件功能不进行重点检查。

## 分层策略

手工测试策略：

涵盖应用及系统接口安全，WEB安全，权限检查，数据存储检查，这些部分都需要通过手工测试来进行。

自动测试策略：

过程中会用到APPSCAN，敏感信息扫描工具，Nessus，PeachFuzzer，NMAP以及NGS Squirrel这些工具做自动化的扫描和测试。

版本源代码需进行安全工具扫描。

## 测试计划

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **版本名称** | **测试时间** | | **测试人员** | **测试地点** | **配套测试的配套版本** | |
| **起始时间** | **结束时间** | **产品名称与版本号** | **版本说明** |
| BI大数据平台 | 16-04-19 | 16-04-28 | 张中维 | 南京 | BI大数据平台 |  |
| BI大数据平台 | 16-04-21 | 16-04-28 | 金雪松 | 南京 | BI大数据平台 |  |

## 自动化策略

目前暂使用公司规定的一些自动化安全测试工具并行安全测试（如Appscan、Nmap、Nessus、PeachFuzz等），安全自动化用例暂未成熟，待后期补充实施。

## 测试工具规划

涵盖所有测试过程中需要用到的工具，在这里列明，并给出获取方式：

|  |  |  |  |
| --- | --- | --- | --- |
| 工具名称 | 作用 | 工具地址账号信息 | 备注 |
| APPSCAN | Web服务器扫描 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| PeachFuzzer | Fuzz模糊测试工具 | https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 | 本地部署，参考附件中的PeachFuzzer测试指导。 |
| Nessus | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| SecureCAT | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NMAP | 端口扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NGS Squirrel | 数据库安全扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| Coverity | 代码静态扫描 | 专门服务器提供扫描，无需个人部署。 |  |
| Fortify | 代码静态扫描 | 专门服务器提供扫描，无需个人部署。 |  |
| 防病毒软件（Symantec、Mcafee、Avira AntiVir、卡巴斯基等） | 病毒扫描 | VMP提供自动扫描功能 |  |
| Burpsuit | 网络通信测试工具 | 单机版，归档地址：  https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 |  |
| 敏感信息扫描工具 | 扫描秒干信息 | 单机版，归档地址：  https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 |  |

# 安全测试策略

## 总体测试策略

### 测试点分析

* 数据清洗入库与数据计算输出；
* 环境检查及相关工具扫描；
* 模块接口与信息传输通道；

涉及模块主要有执行网关、FusionInsight、DataPush、DataLoad以及NFS。

重点测试敏感数据是否加密存储、传输，用户鉴权，等安全红线测试用例，并使用安全工具对操作系统漏洞、代码、、服务端口等进行扫描和检查，并使用codenomicon fuzz工具对SSH V2标准协议进行fuzz测试。

### 高风险模块分析

DataPush/DataLoad：主要负责推送数据的缓存及入库具体操作，及主要的接口和业务逻辑，需重点进行协议与接口防攻击，管理通道以及敏感数据安全方面的测试

NFS：数据通道配置在NFS上，作为临时数据存储的地方。

执行网关：TCC通过执行存储在执行网关上的脚本，向业务服务器、NFS以及hive提交数据推送、数据入库以及计算等任务，需重点进行协议与接口防攻击，管理通道以及敏感数据安全方面的测试

### 继承特性的安全测试策略

自研部件需要全部测试，因此这部分的继承特性分析不涉及，部分第三方安全软件可参考公司相关规范处理。

### 安全基线用例集覆盖策略

《云业务安全测试基线用例集V1.1》以公司产品网络安全红线落地解读及指导2.0、消费者BG隐私设计规范V1.0要求为基准，并借鉴安全能力中心《滥用用例库V1.1》、《通用软件基础安全测试用例 v1.0》、《开源及第三方软件网络安全测试用例》、《安全网上问题案例集ICSL》。

目前云业务产品的安全基线用例库经过内部评审已经定稿，服务器全部用例涵盖如下维度：安全红线要求、非安全红线要求，以及服务器公共安全测试用例。红线部分也包括了隐私保护、未公开接口、访问通道控制、软件完整性保护、敏感数据与加密保护、日志审计、操作系统加固与防病毒、Web安全、产品开发发布和安装安全、数据库加固和口令安全。参照此基线进行该版本服务器全部用例的安全测试，保证产品符合公司及消费者云服务网络安全要求。

### 测试风险分析

测试能力：目前安全测试方面，对一些工具掌握不够完全，投入时间也不足；目前只能针对安全红线测试用例做防御性的测试设计和测试执行，渗透测试等测试能力有待提升。

### **网上问题分析**

**BI大数据平台暂无安全方面的现网问题，针对前期送测过ICSL的其他业务版本所发现的问题，以及产品相关的网上问题，验证在当前BI大数据平台**BI DSPT 1.0.3.101**版本是否存在。案例集涵盖在：*https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/01 ICSL送测/03 送测结果***

**针对OpenSSL心脏滴血漏洞进行OpenSSL的版本号排查，信息根据：**

**受影响：**

* **OpenSSL 1.0.2-beta**
* **OpenSSL 1.0.1 - OpenSSL 1.0.1f**

**不受影响：**

* **OpenSSL 1.0.2-beta2（将来版本）**
* **OpenSSL 1.0.1g**
* **OpenSSL 1.0.0（及1.0.0的分支版本）**

**OpenSSL 0.9.8（及0.9.8的分支版本）**

### **老代码和依赖的平台代码测试策略分析**

**BI大数据平台代码都是基于系统需求业务框架下的实现，不区分平台和老代码，需要做一致性的安全风险排查。主要包括代码中的注释，加密算法，敏感信息，硬编码的一些信息等等，会在测试过程中体现。**

### **Fuzz测试策略**

本版本测试根据《Fuzzing测试指南》的要求确定需要测试的协议为标准SSH V2协议。本版本FUZZ测试使用的工具：codenomicon。需要对系统的外部交互SSH V2协议重点进行FUZZ测试。

### **威胁建模分析和测试策略**

#### 业务服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 业务服务器 | |
| 元素概述 | 各个业务的服务器，对外提供服务，对内以数据推送的方式和数据平台交互，主要为BI数据平台提供数据来源。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：高**。  1.系统被仿冒后，会推送错误的数据到BI平台，错误的数据部分会被清洗，即使部分数据传输到数据通道，只会造成数据无法入库。  2.被仿冒后不断往BI内部推送数据，造成BI文件服务器宕机，或者推送错误数据，导致产生错误的计算结果。  **可能性评估 低** |
| 已有消减措施 | 1.通过白名单机制，保证非法IP无法完成数据推送  2.已被授权进行数据推送的用户，生成SSH协议的公钥和私钥，公钥存储在BI平台内部的数据通道上，推送的用户在进行数据推送时使用私钥进行认证。生成密钥对的口令通过加密方式存储在配置文件中。 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | 风险：中  影响：中。业务侧否认进行了错误的配置，推送超量数据或者重复数据或者推送失败，导致数据通道磁盘满载，无法接收其他业务数据或者导致数据入库任务无法执行。  可能性：低 |
| 已有消减措施 | 1.通过操作系统日志可以记录用户的操作记录 |
| 建议消减措施 | 根据公司审计日志规范修改工具审计日志格式 |
| 产品落地计划 | NA |

#### TCC

|  |  |  |
| --- | --- | --- |
| 元素名称 | TCC | |
| 元素概述 | Task Control Center，自研的任务调度和控制系统。开发人员通过web页面配置任务的类型、执行周期等。TCC通过执行配置再网关机上的脚本执行各类任务。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：高。**如果TCC系统被仿冒，可能会执行需要大量资源的任务或者执行获取用户隐私的任务。  **可能性评估：低** |
| 已有消减措施 | 1.TCC部署在BI内部机房，有专用网络保护  2.TCC和执行网关通过SSH进行身份认证（认证方式为公钥认证），SSH协议版本号为V2.0 ，算法包括aes128-ctr,aes192-ctr,aes256-ctr |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：中**  **影响：中。**开发人员否认自己的操作，有日志记录，抵赖影响较小。  **可能性评估：小** |
| 已有消减措施 | 2. TCC日志格式为：2016-05-16 15:31:48.083 INFO - - info() Thread-76730 [listerner[com.huawei.platform.tcc.service.impl.TccServiceImpl@3d62ba]](mailto:listerner[com.huawei.platform.tcc.service.impl.TccServiceImpl@3d62ba]) needs 2 ms to process Event[UPDATE\_JOB\_IDS,[[Ljava.lang.Object;@747174b2](mailto:[Ljava.lang.Object;@747174b2),[com.huawei.platform.tcc.SSH.ResultProcess@4d74f5d5]!](mailto:com.huawei.platform.tcc.SSH.ResultProcess@4d74f5d5]!) 不满足公司审计日志要求 |
| 建议消减措施 | TCC审计日志应该由执行网关机上的壳程序输出，从而可以在BI内部追踪用户的操作。修改TCC审计日志为满足公司审计要求的格式。 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |

#### 文件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 文件服务器 | |
| 元素概述 | 数据开发人员通过使用Hive计算的结果，进行报表、群体用户画像等数据产的开发 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：中**  **影响：高**  数据开发人员被仿冒后，可能导致大量用户隐私数据被泄露，影响较大  **可能性评估：可能性较小**  1.VPN控制特定的开发人员能否访问内网机房  2.操作系统用户权限控制，有SSH协议做认证  3.DataPush工具提供日志记录 |
| 已有消减措施 | 1.安全  1.1VPN控制特定的开发人员能否访问内网机房  1.2.操作系统用户权限控制，有SSH协议做认证(补充协议等信息)  1.3.DataPush工具提供日志记录  2.隐私 |
| 建议消减措施 | 实验室继承办公室的意见：  1) BI具有回传数据到中国的能力  2) 什么数据通过BI回传需要走备案通过，通过后才能回传  3) 在回传前数据还留着欧洲  4） 在后续版本中完善回传方案 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：中。**  **可能性评估：低** |
| 已有消减措施 | 1. datapush日志记录文件推送行为   2. 操作系统日志记录OS用户行为 |
| 建议消减措施 |  |
| 产品落地计划 |  |

#### 运维人员

|  |  |  |
| --- | --- | --- |
| 元素名称 | 运维人员 | |
| 元素概述 | 运维人员通过NFSzabbix监控NFS端口服务的状态 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：低**  运维人员被仿冒后，只能观察到NFS服务状态，无法获取到存储在NFS上的数据  **可能性评估：可能性较小**  VPN控制特定的开发人员能否访问内网机房 |
| 已有消减措施 | 1.zabbix有密码强度校验  2.运维人员只能监控状态，不能修改 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：低。**  **可能性评估：低** |
| 已有消减措施 | Zabbix有审计日志 |
| 建议消减措施 |  |
| 产品落地计划 |  |

#### 业务服务器⇒ /NFS/DataIn

|  |  |  |
| --- | --- | --- |
| 元素名称 | 业务服务器⇒/NFS/DataIn | |
| 元素概述 | 业务服务器通过配置定时的数据推送任务，对数据进行初步的清理和转换，推送数据到数据通道的/NFS/DataIn目录下，等待数据入BI数据仓库 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中。**数据被篡改会导致数据无法入库或者计算任务执行异常，或者得到错误的计算结果。  **可能性评估：**  接入华为机房对推送数据流出口进行劫持篡改数据流可能性较小 |
| 已有消减措施 | 1.业务服务器部署在华为专有机房，必须具有vpn才能接入机房和获取数据流  2.推送的数据进行打包加密处理，即使劫持到也无法解压 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：大**  此数据流的数据如果泄露，可能会泄露用户隐私数据，影响较大  **可能性评估：**  接入华为机房进行网络抓包分析，数据加密压缩，通过安全的ssh协议传输，泄露可能小较小 |
| 已有消减措施 | 1.接入机房需要VPN权限  2.数据加密压缩  3.ssh协议传输，保证数据传输安全 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：**中。数据推送工具异常会导致数据无法推送到数据通道，周期任务无法执行  **可能性评估：中**  1.推送工具所在业务服务器异常，到时数据无法推送  2.业务服务器和数据通道之间的网络异常  3.数据通道文件服务器异常 |
| 已有消减措施 | 1.数据推送异常有告警机制，运维人员可快速得到通知进行处理  2.数据重新推送机制，数据推送失败会再次推送 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### /NFS/DataIn⇒FusionInsight

|  |  |  |
| --- | --- | --- |
| 元素名称 | /NFS/DataIn⇒FusionInsight | |
| 元素概述 | 临时数据通道的数据通过入库工具，被加载到FusionInsight的Hive表在HDFS上的目录下 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：低**  数据被篡改会导致计算任务执行失败或者结果不正确。  **可能性评估：低**  1.数据从数据通道加载到HDFS上，使用https等安全的通信协议  2.加载数据的用户身份通过kerbros进行认证 |
| 已有消减措施 | 1.需要VPN权限才能访问部门内部机房  2.机房服务器需要主管审批才能访问  3.FusionInsight内部的数据加密传输机制保证 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**。信息泄露会涉及到用户的隐私数据，影响较大  **可能性评估：低** |
| 已有消减措施 | 1.需要VPN权限才能访问部门内部机房  2.机房服务器需要主管审批才能访问  3.FusionInsight内部的数据加密传输机制保证 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：低**。数据无法加载到数据仓库，导致周期任务无法执行。  **可能性评估：中**  1.DataLoad工具所在服务器异常  2.FusionInsight HDFS或者hive组件无法访问  3.Dataload工具到FusionInsight网络异常 |
| 已有消减措施 | 1.数据入库异常有告警机制，运维人员可快速得到通知进行处理 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### FusionInsight⇒/NFS/DataOut

|  |  |  |
| --- | --- | --- |
| 元素名称 | FusionInsight⇒/NFS/DataOut | |
| 元素概述 | FusionInsight中的数据仓库计算结果导出到临时数据通道的/NFS/DataOut目录，等待推送回国内的数据开发人员处 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**。国内数据开发人员看不到本周期的计算结果，无法进行报表开发或者画像开发；或者看到错误的计算结果，影响产品决策。  **可能性评估：**可能性较小 |
| 已有消减措施 | 1.需要VPN权限才能访问部门内部机房  2.机房服务器需要主管审批才能访问  3.FusionInsight内部的数据加密传输机制保证 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  信息泄露会涉及到用户的隐私数据，影响较大  **可能性评估：**低 |
| 已有消减措施 | 1.需要VPN权限才能访问部门内部机房  2.机房服务器需要主管审批才能访问  3.FusionInsight内部的数据加密传输机制保证 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：中。**国内数据开发人员看不到本周期的计算结果，无法进行报表开发或者画像开发  **可能性评估：高**  1.FusionInsight组件服务异常  2.数据通道服务器异常  3.数据通道和FusionInsight之间网络异常 |
| 已有消减措施 | 1.FusionInsight提供告警机制，可及时通知运维和开发人员进行处理  2.机房网络、主机以及端口提供监控告警机制 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### FusionInsight⇔执行网关

|  |  |  |
| --- | --- | --- |
| 元素名称 | FusionInsight⇔执行网关 | |
| 元素概述 | 执行网关机提交Hive脚本到FusionInsight中的Hive组件执行计算任务，Hive执行结果或者日志返回网关机 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**  脚本被篡改，会导致危险的计算任务被执行，影响较大  **可能性评估：低**  1.需要VPN权限才能访问部门内部机房  3.FusionInsight客户端和服务器通信进过kerbros认证，数据加密传输 |
| 已有消减措施 | 1.网关机所在机房的接入需要VPN权限  2.FusionInsight内部机制保证数据安全传输 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  1.泄露hive表结构信息  2．执行结果返回执行网关的数据可能泄露用户隐私数据  **可能性评估：中**  通过网络嗅探抓包分析 |
| 已有消减措施 | 1．脚本通过FusionInsight内部安全加密机制提交到hive  2. 网关机访问权限审批机制  3. 具有VPN权限的用户才能访问部门内机机房 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：中**。无法提交任务到Hive执行计算任务，导致报表等数据产品不能正常使用和开发。  **可能性评估：高**  1.FusionInsight组件异常  2.执行网关所在的文件服务器异常  3.执行网关和FusionInsight之间的网络异常 |
| 已有消减措施 | 1.运维监控服务器状态  2.FusionInsight提供Hive服务状态告警 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### /NFS/DataOut⇒文件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | DataOut⇒数据开发人员 | |
| 元素概述 | 数据通道上的DataOut目录的数据通过定时的数据推送任务推送回国内的数据开发人员处，进行数据产品的开发和测试。 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：低**。计算结果被篡改，会导致数据开发人员获取到错误的计算结果，影响数据产品的开发  **可能性评估：低**  1.数据通道服务器的访问权限需要审批  2.ssh协议保证数据安全传输（协议版本号和算法） |
| 已有消减措施 | 1.数据通道生成SSH协议密钥对，公钥存储在数据开发人员所在的服务器，通过建立安全的ssh通道进行数据传输。SSH协议版本号为V2.0 ，算法包括aes128-ctr,aes192-ctr,aes256-ctr |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：大。**如果计算结果中包含了用户隐私数据，则影响较大  **可能性评估：** |
| 已有消减措施 | 1.数据通道生成SSH协议密钥对，公钥存储在数据开发人员所在的服务器，通过建立安全的ssh通道进行数据传输。SSH协议版本号为V2.0 ，算法包括aes128-ctr,aes192-ctr,aes256-ctr |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：中**  **可能性评估：高**  服务器或者服务器之间的网络异常，可能导致数据无法推送到数据开发人员处 |
| 已有消减措施 | 1.运维监控服务器状态和机房网络状态，及时通知开发人员进行处理 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### NFS⇒运维人员

|  |  |  |
| --- | --- | --- |
| 元素名称 | NFS⇒运维人员 | |
| 元素概述 | 运维人员通过监控NFS服务器的端口来判断NFS服务是否正常 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：低**  **可能性评估：低**  数据根据linux操作系统用户权限管理进行保护 |
| 已有消减措施 | 1.具有VPN权限才能访问部门内部机房 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高。**涉及用户隐私的数据可能被泄露  **可能性评估：**  数据可能通过NFS的端口泄露 |
| 已有消减措施 | 1.具有VPN权限才能访问部门内部机房  2.NFS的端口不对外开放，由运维人员管理 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：中**  **可能性评估：中**  1.NFS组件异常  2.NFS服务网络异常 |
| 已有消减措施 | 1.运维监控服务器和网络状态 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### DataPush

|  |  |  |
| --- | --- | --- |
| 元素名称 | DataPush | |
| 元素概述 | 把FusionInsight的计算结果从数据通道的/NFS/DataOut目录推送到数据开发人员 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：中**  1.仿冒DataPush，可能导致计算结果被推送到危险的地方  2.仿冒DataPush，可能导致业务服务器推送不符合要求的数据  **可能性评估：低**  1.VPN权限保证特定用户才能访问机房 |
| 已有消减措施 | 1.VPN权限审批机制保证特定用户才能访问BI内部机房 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：高**  DataPush被篡改后会导致数据无法推送或者推送错误的数据到数据开发人员处  **可能性评估：**  DataPush的配置文件被篡改，可能性较大 |
| 已有消减措施 | 1.申请VPN权限才能访问BI内部机房  2.业务服务器访问权限控制  3.ssh密钥进行访问认证和加密数据传输 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：高。**  **可能性评估：**  开发人员抵赖自己的操作，会有操作系统日志进行回溯和审查。 |
| 已有消减措施 |  |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  如果计算结果中包含了用户个人数据，那么用户数据会泄露，影响较大  **可能性评估：**  获取服务器权限，修改DataPush配置文件，可能性较小 |
| 已有消减措施 | 1.VPN权限访问机房  2.业务服务器访问权限控制 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：低**  计算结果数据无法推送到国内数据开发人员处，影响数据产品的开发和测试  **可能性评估：**  DataPush所在服务器或者网络故障。 |
| 已有消减措施 | 1.运维对机房内部的服务器和网络进行监控，发现异常及时通知开发人员进行处理 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 特权提升（E） | 风险（Risk） | **风险等级：高**  **影响：高**  1.运行DataPush的进程获取root权限后，可能导致数据被推送到不该服务器，导致用户隐私数据泄露  2.不涉及数据库权限提升  **可能性评估：低**  获取root权限需要安全部门主管的审批 |
| 已有消减措施 |  |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### 执行网关

|  |  |  |
| --- | --- | --- |
| 元素名称 | 执行网关 | |
| 元素概述 | TCC通过执行存储在执行网关上的脚本，向数据通道、FusionInsight提交数据推送或者计算任务。 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：高**  **被仿冒后，会执行有风险的任务，导致用户隐私数据泄露**  **可能性评估：**  可能性较小 |
| 已有消减措施 | 1.VPN权限访问国内机房  2.OS用户权限审批 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**  篡改网关机上的脚本，可能会提交有风险的计算任务，把用户隐私数据输出到有风险的目录，导致用户隐私数据泄露  可能性较小 |
| 已有消减措施 | 1.VPN权限访问国内机房  2.OS用户权限审批 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：中**  **影响：高**  **可能性评估：**  **中** |
| 已有消减措施 |  |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  存储在网关机上的执行脚本泄露，会导致hive表信息泄露  **可能性评估：**  可能性较小 |
| 已有消减措施 | 1.VPN权限访问国内机房  2.OS用户权限审批 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：中**  各项任务无法提交，影响报表、画像等产品依赖的数据  **可能性评估：**  1.执行网关所在服务器异常  2.执行网关和FusionInsight之间的网络异常 |
| 已有消减措施 | 运维监控BI内部机房服务器和网络的运行状态，如果有异常，及时进行处理 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：中**  **可能性评估：**  1.执行任务的客户端端进程获取root权限后，可能执行不属于该用户执行的脚本任务，导致计算周期混乱，计算结果出错  2.执行任务的客户端进程操作HIVE的权限提升后，可能导致客户端访问该用户本没有权限的表和数据 |
| 已有消减措施 | 依赖FusionInsight保障机制 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### NFS

|  |  |  |
| --- | --- | --- |
| 元素名称 | NFS | |
| 元素概述 | 数据通道配置再在NFS上，作为临时数据存储的地方 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：中**  **影响：中**  **可能性评估：低** |
| 已有消减措施 |  |
| 建议消减措施 | 客户端挂载NFS，需要增加NFS客户端对NFS服务端的认证 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：低**  数据被篡改会导致数据无法入库或者hive任务计算出错误的结果 |
| 已有消减措施 |  |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：高**  **影响：高**  **可能性评估：操作系统日志可以追溯用户对NFS的操作** |
| 已有消减措施 |  |
| 建议消减措施 | 启动NFS审计日志功能，对用户操作进行监控 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  存储在NFS上的数据泄露，会导致用户隐私数据泄露  **可能性评估：**  可能性较小 |
| 已有消减措施 | 1.VPN权限访问国内机房  2.OS用户权限审批 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：中**  数据无法完成推动，结果文件无法推送回国内  **可能性评估：**   1. NFS所在的服务器或者网络出现异常 2. 可靠性保证 |
| 已有消减措施 | 运维监控BI内部机房服务器和网络的运行状态，如果有异常，及时进行处理 |
| 建议消减措施 | NFS具有单机宕机风险，需要实现NFS高可用设计 |
| 产品落地计划 |  |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：中**  **可能性评估：NFS运行操作系统账号** |
| 已有消减措施 | 壳程序脚本权限（550） |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |

#### /NFS/DataIn

|  |  |  |
| --- | --- | --- |
| 元素名称 | /NFS/DataIn | |
| 元素概述 | 业务服务器推送数据后，数据在数据通道上的临时存放路径 | |
| 威胁 | TRID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**  数据被篡改后，执行数据入库任务报错或者入库错误的数据，导致开发人员获取不到数据或者获取到错误的计算结果  **可能性评估：**  1.具有VPN权限才能访问BI内部机房  2.访问数据通道的服务器权限，需要审批 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员使用vpn登录到本地系统才能访问（统一由运维作为入口，如果统一由运维操作，可以去掉vpn相关内容）  2. 只有运行对应业务的用户才能访问，其他linux用户无法访问(文件，目录，都是什么权限，针对篡改进行权限设置说明，去掉写权限) |
| 建议消减措施 | 1.数据通道datain目录的数据定期清理，减少数据通道数据量，降低NFS服务器磁盘空间使用  2.加入数据质量监控，防止数据量猛增导致NFS服务不可用 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：低**  **可能性：低** |
| 已有消减措施 |  |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高**  存放了用户的隐私数据，一旦泄露，影响较大  **可能性评估：**  vpn账号和对应的linux用户密码泄露导致恶意用户通过ssh接入服务器查看文件信息  可能非常小 |
| 已有消减措施 | 参考篡改已有消减措施 |
| 建议消减措施 | **拷贝不需要读权限，可以去掉** |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：中**  数据无法推送，导致数据无法入库、计算和回传，影响数据开发人员进行数据产品开发  **可能性评估：高**  数据通道服务器异常或者网络异常 |
| 已有消减措施 | 运维监控BI内部机房服务器和网络的运行状态，如果有异常，及时进行处理 |
| 建议消减措施 | 1.数据通道datain目录的数据定期清理，减少数据通道数据量，降低NFS服务器磁盘空间使用  2.加入数据质量监控，防止数据量猛增导致NFS服务不可用 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |

#### /NFS/Share

|  |  |  |
| --- | --- | --- |
| 元素名称 | /NFS/Share | |
| 元素概述 | 执行网关节点存储的执行脚本和执行工具 | |
| 威胁 | TRID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**  篡改后导致各类任务无法执行或者执行的结果不正确  **可能性评估：**  可能性较小 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员使用vpn登录才能操作  2. 只有运行对应业务的用户才能访问，其他linux用户无法访问 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **不分析：可接受的风险** |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：低**  任务执行的相关信息会丢失，但是用户数据不会丢失。影响较小  **可能性评估：**  可能非常小 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员使用vpn登录才能操作  2. 只有运行对应业务的用户才能访问，其他linux用户无法访问 |
| 建议消减措施 | 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：中**  无法执行各类任务  **可能性评估：高**  Share目录所在的服务器或者网络环境异常 |
| 已有消减措施 | NFS具有单机宕机风险，需要实现NFS高可用设计 |
| 建议消减措施 | 无 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |

#### /NFS/DataOut

|  |  |  |
| --- | --- | --- |
| 元素名称 | /NFS/DataOut | |
| 元素概述 | 存储hive的计算结果，通过启动推送任务把结果回传到数据开发人员 | |
| 威胁 | TRID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：中**  待入库的数据一旦被篡改，将导致业务流程异常或数据异常，数据无法入库或者  **可能性评估：**  可能性非常低 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员使用vpn登录才能操作  2. 只有运行对应业务的用户才能访问，其他linux用户无法访问 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. NA |
| 抵赖（R） | 风险（Risk） | **风险等级：中**  **影响：中**  **可能性：中** |
| 已有消减措施 | NA |
| 建议消减措施 | 启动NFS审计日志功能，对用户操作进行监控 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：高。**DataOut中如果存储了用户隐私数据，将导致隐私数据泄露，影响很大。  **可能性评估：**  可能性非常低 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员使用vpn登录才能操作  2. 只有运行对应业务的用户才能访问，其他linux用户无法访问 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：中。**导致数据无法推送到开发人员侧，无法完成数据产品开发。  **可能性评估：**  数据通道所在的服务器或者网络出现异常 |
| 已有消减措施 |  |
| 建议消减措施 | 1. 1.数据通道dataout目录的数据定期清理，减少数据通道数据量，降低NFS服务器磁盘空间使用 2. 2.加入数据质量监控，防止数据量猛增导致NFS服务不可用 |
| 产品落地计划 | 20160810-DSPT 1.0.3.400 |

**本次测试将按照《BI大数据平台TM安全测试方案\_V0.3》第5章描述的测试方法和内容对威胁分析中各种威胁和消减措施进行测试。**

## SDV安全测试策略

#### 测试重点

重点测试协议与接口安全、敏感数据是否加密存储、传输，用户身份验证等安全红线测试用例，并使用安全工具对操作系统、代码、端口等进行扫描和检查，并使用fuzz工具对标准ssh v2协议进行fuzz测试。本次是全量覆盖安全测试，跟业务团队做的沟通结果是在SDV阶段，覆盖云安全基线用例集。

#### 入口准则

入口条件，开发提供如下交付件。

|  |  |
| --- | --- |
| **序号** | **交付件名称** |
|
| 1 | 特性列表 |
| 2 | 需求设计说明书 |
| 3 | 安全性威胁分析及需求说明书 |
| 4 | 安全设计说明书 |
| 5 | 安全及隐私设计检视Checklist（含共性设计问题） |
| 6 | 差异化分析说明书 |
| 7 | 代码静态扫描报告 |
| 8 | 代码安全检视报告 |
| 9 | AppScan扫描报告 |
| 10 | Fuzz测试结果以及问题跟踪记录 |
| 11 | 通信矩阵 |
| 12 | 安全配置/加固指南 |
| 13 | 安全操作维护手册 |
| 14 | 防病毒部署指南 |
| 15 | 安全技术白皮书 |
| 16 | 业务安全相关文件信息说明 |
| 17 | 第三方代码开源认证报告 |
| 18 | 开源及第三方软件使用申请单 |
| 19 | 源代码 |
| 20 | 安全红线&隐私设计自检 |
| 21 | 安全测试策略 |
| 22 | 安全测试方案 |
| 23 | 安全测试用例 |

#### 出口准则

经过SDV测试，业务团队在经过测试后发现的所能发现的所有安全问题，在开发修改后，可以闭环，达到SDV测试结束的条件（无AB类安全红线问题遗留），可以结束SDV的安全测试。

## SIT安全测试策略

#### 测试重点

经过SDV的安全红线基线用例集覆盖测试，已经完成红线排查和和安全问题闭环。业务团队在SIT阶段测试的重点为核心代码走读，解读敏感接口的流程，对于算法的具体实现进行排查，这也是之前在线升级送测暴露的一些问题。

#### 入口准则

a.SDV安全测试结束。

b.发现的安全问题闭环，无AB类安全红线问题遗留。

#### 出口准则

a.完成SIT制定的测试工作和测试用例。

b.发现的问题闭环，无AB类安全红线问题遗留，无CVSS打分大于7分的严重级别问题遗留。

## SVT安全测试策略

华为内部自运营系统，暂不涉及SVT测试。

# 参考资料清单

## 安全基线用例集，构建于TMSS服务器

## Web安全测试规范\_V1.4.docx