|  |  |  |
| --- | --- | --- |
| Huawei Technologies Co. Ltd.  华为技术有限公司 | 产品名称：BI大数据平台 | 密级 |
| 产品版本： | 内部公开 |
| BI DSPT 1.0.3.100 | 共18页 |

BI BigData Platform Safety Test Report

BI大数据平台安全性测试与评估报告

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 | 张中维/zwx318675 | Date  日期 | 2016-04-29 |
| Reviewed by  评审人 |  | Date  日期 |  |
| Approved by  批准 |  | Date  日期 |  |



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

All rights reserved  
版权所有 侵权必究

Revision Record 修订记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date  日期 | Revision Version  修订 版本 | CR ID / Defect ID CR号 | Sec No.  修改 章节 | Change Description  修改描述 | Author  作者 |
| 2016/04/29 | 1.00 |  |  | 初稿完成 | 张中维/zwx318675 |
|  |  |  |  |  |  |

Catalog 目 录

[1 安全性测试背景 5](#_Toc449710720)

[1.1 测试目的 5](#_Toc449710721)

[1.2 测试对象 5](#_Toc449710722)

[1.3 测试环境描述 5](#_Toc449710723)

[1.3.1 测试组网 5](#_Toc449710724)

[1.3.2 测试工具 6](#_Toc449710725)

[2 测试执行情况及结果分析 7](#_Toc449710726)

[3 产品安全性质量评估 8](#_Toc449710727)

[3.1 总体评估结论 8](#_Toc449710728)

[3.2 产品安全性总体质量评估 8](#_Toc449710729)

[3.3 产品安全性质量标准评估 9](#_Toc449710730)

[3.3.1 监听端口与防止非法监听 9](#_Toc449710731)

[3.3.2 隐私保护 9](#_Toc449710732)

[3.3.3 禁止未公开接口 10](#_Toc449710733)

[3.3.4 访问通道控制 10](#_Toc449710734)

[3.3.5 软件完整性保护 11](#_Toc449710735)

[3.3.6 敏感数据与加密保护 11](#_Toc449710736)

[3.3.7 日志审计 12](#_Toc449710737)

[3.3.8 操作系统加固与防病毒 13](#_Toc449710738)

[3.3.9 协议与接口防攻击 13](#_Toc449710739)

[3.3.10 Web安全 13](#_Toc449710740)

[3.3.11 产品开发、发布和安装安全 14](#_Toc449710741)

[3.3.12 数据库加固 15](#_Toc449710742)

[3.3.13 口令安全 15](#_Toc449710743)

[3.4 安全设计改进建议 15](#_Toc449710744)

[4 产品安全性问题/风险汇总和跟踪 16](#_Toc449710745)

[5 测试结论 17](#_Toc449710746)

[6 附件 17](#_Toc449710747)

[6.1 端口扫描结果 17](#_Toc449710748)

[6.2 安全漏洞扫描结果 17](#_Toc449710749)

[6.3 Web系统漏洞扫描结果 17](#_Toc449710750)

[6.4 Codenomicon Defensics扫描结果 17](#_Toc449710751)

[6.5 防毒软件扫描结果 17](#_Toc449710752)

[6.6 安全红线自检报告及举证材料 18](#_Toc449710753)

[6.7 源代码静态安全扫描分析报告 18](#_Toc449710754)

[6.8 通信矩阵 18](#_Toc449710755)

BI BigData Platform Safety Test Report

BI大数据平台安全性测试与评估报告

Keywords 关键词：BI大数据平台 安全测试 网络安全 脆弱性

Abstract 摘要：本文档详细描述了安全测试人员在BI大数据平台安全测试过程中发现的产品安全脆弱性，对BI大数据平台的安全状况进行全面的分析，并给出整改建议。

List of abbreviations 缩略语清单：

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| DFNS | Design For Network Security | 网络安全性设计 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 安全性测试背景

## 测试目的

针对BI大数据平台各服务组件，通过安全测试，验证产品安全质量，发现系统中存在的安全脆弱性（Vulnerability）与风险（Risk），为产品的安全改进提供切实的依据，推动产品完成安全问题整改，从而提高产品安全性。此次主要利用APPSCAN、Nessus、Codenomicon、Nmap、NGS等工具扫描BI大数据平台相关组件，发现软件的安全漏洞。

## 测试对象

|  |  |
| --- | --- |
| 产品名称 | BI大数据平台 |
| 产品版本 | BI DSPT 1.0.3.100 |
| 详细版本号 |  |

测试时间：2016年04月18日——2016年04月28日

测试地点：南京

测试人员：张中维/wx318675

金雪松/j00165946

陆璐/wx290483

## 测试环境描述

### 测试组网

本次测试的主要组网环境和业务配置：



由开发部署好BI大数据平台所有待测组件，并确认系统各功能模块业务部署正常，通过vpn接入Nginx代理服务器对数据平台进行各项安全测试。

### 测试工具

测试过程中使用的主要工具：

|  |  |  |  |
| --- | --- | --- | --- |
| **测试工具** | 用途 | 厂商 | 版本 |
| Nessus | 漏洞扫描工具，用于扫描网中中的服务器、计算机漏洞，可用于黑客攻击前的信息收集。 | Tenable Network Security, Inc. | Nessus Version：6.3.7 |
| Nmap | 网络协议分析工具，可用于抓取及分析网络中的计算机及其他网络设备之间的所有通讯数据。 | 开源 | 6.47 |
| Codenomicon  Defensics | 协议级健壮性和攻击测试 | Codenomicon | 11.7.1 |
| APPSCAN | Rational AppScan是IBM公司的Web应用安全测试工具 | IBM | V9.0.2 |
| Burp Suite | Web应用攻击测试平台 | portswigger | V1.6 |
| Peach | 协议模糊测试工具 | Huawei | 3.4.24 |
| Attacker | Attacker用于模拟网络中存在的多种DDOS攻击，模拟攻击网络安全设备保护的网络资源 | Huawei | V1.0.8.1 |
| Search and replace | 用于排查代码、文件中的非安全函数和敏感信息 | 开源 | 5.0 |
| Coverity Integrity Center | 静态扫描工具 | Coverity | 公司平台 |
| Fortify Static Code Analyzer | 静态的、白盒的软件源代码安全测试工具。 | HP | 公司平台 |
| Symantec Endpoint Protection | 病毒扫描工具 | 赛门铁克 | 公司平台(VMP) |
| OfficeScan | 趋势科技 |
| McAfee VirusScan | McAfee |
| Avira AntiVir | Avira |
| 卡巴斯基(Kav) | 卡巴斯基 |

# 测试执行情况及结果分析

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 统计 | 总测试  用例数 | 实际测试的用例数 | Passed项 | Failed项 | Blocked项 | Unavailable项 | Investigated项 | 无需测试用例数 |
| 云业务安全测试基线用例集V1.1 | 970 | 413 | 407 | 6 | 557 |  |  |  |
| 总数 |  |  |  |  |  |  |  |  |
| 百分比 |  |  |  |  |  |  |  |  |

其中：

Passed 用例执行成功

Failed　用例执行结果未通过或者测试执行过程中遇到其它与本用例无关的失效事件

Block　产品不涉及

Unavailable由于软件本身以外，如环境、工具、物料、时间、人力资源等因素导致用例未执行

Investigated　用例部分执行未通过（用例主体部分执行通过）

安全测试用例及执行结果如下：



# 产品安全性质量评估

## 总体评估结论

网络安全测试覆盖网络安全红线/产品线网络安全测试基线涉及BI大数据平台的方面，包含禁止未公开接口、访问通道控制、web安全、软件完整性保护、敏感数据与加密保护、日志审计、操作系统加固和防病毒、协议与接口防攻击、产品开发、发布和安装安全、口令安全、安全资料，覆盖总体安全测试策略中的所有安全需求。

本次测试发现安全问题致命问题0个，严重问题1个，一般问题0个，提示问题5个。其中1个严重问题为Appscan扫描发现，开发已经在分析解决并同步安全组备案流程，5个提示问题部分已经修改，遗留3个提示问题（服务器文件权限待严格设置2个；日志文件删除后自动生成1个）。

经过安全专项测试、手工测试、Fuzz测试、消减措施测试，从测试结果来看，系统在设计、开发、测试上对网络安全考虑充分，测试充分，测试执行覆盖率达到100％，针对遗留问题经过评估风险可控， BI大数据平台产品网络安全测试通过。

## 产品安全性总体质量评估

通过实测和检查，BI大数据平台BI DSPT 1.0.3.100版本在TR5点完全达成公司DFNS质量属性标准/安全红线质量要求。

|  |  |  |
| --- | --- | --- |
| **安全属性** | **结论**  **(满足/不满足/不涉及)** | **主要问题描述及涉及的要求级别**  **（A1/A2/B）** |
| 监听接口及防止非法监听 | 不涉及 |  |
| 隐私保护 | 不涉及 |  |
| WEB应用安全 | 不满足 | 使用AppScan扫描有高风险问题，待修改 |
| 安全资料 | 满足 |  |
| 操作系统安全与防病毒 | 满足 | 使用Nessus扫描不存在风险，只有部分提示信息 |
| 访问通道控制 | 满足 |  |
| 禁止未公开接口 | 满足 |  |
| 口令安全 | 不满足 | 服务器认证密码复杂度待修改 |
| 产品开发、发布与安装安全 | 满足 |  |
| 敏感数据与加密保护 | 不满足 | 部分业务脚本、日志、配置文件权限需按规范设置 |
| 日志审计 | 不满足 | 日志删除后自动生成有异常情况 |
| 软件完整性保护 | 满足 | 实现软件完整性校验。 |
| 协议与防攻击 | 满足 | 完成SSH V2协议的Fuzz测试，测试通过，部分问题为网络延迟导致，不存在安全风险。 |
| 数据库安全 | 不涉及 |  |

## 产品安全性质量标准评估

从安全红线的角度评估版本的目标达成情况。

根据安全红线检查Checklist，分不同测试项，针对各测试评估点给出评估结果和说明，以支撑安全红线目标达成情况的结论。

### 监听端口与防止非法监听

BI大数据平台BI DSPT 1.0.3.100版本不涉及监听功能。

### 隐私保护

|  |  |  |
| --- | --- | --- |
| **测试要点** | **评估结果** | **说明** |
| 对于数据控制者，收集个人数据必须要获得数据主体的授权 | 不涉及 |  |
| 个人数据收集范围、使用目的不得超出隐私声明 | 不涉及 |  |
| 在B/S系统中，如果提交的数据中包含个人数据，则禁止使用Get方式提交个人数据 | 不涉及 |  |
| 产品须对本地存储的个人数据提供适当的安全保护机制，如认证、授权、加密、日志等 | 满足 | 服务器端存放的数据经过安全加密存放在数据库内，存在认证、鉴权和日志等安全保护 |
| 对于数据控制者，提供数据主体录入个人数据功能时，必须提供查询和更新相应个人数据的机制 | 不涉及 |  |
| 对于数据处理者，出于定位问题目的，如需将个人数据拿出客户网络，应提供对其中包含的个人数据进行过滤或匿名化处理的机制或指导 | 满足 | 个人数据过滤后不会包含客户敏感数据 |

### 禁止未公开接口

|  |  |  |
| --- | --- | --- |
| **测试要点** | **评估**  **结果** | **说明** |
| 5.1.1 禁止存在任何“未公开接口”：  1）禁止存在可绕过系统安全机制（认证、权限控制、日志记录）对系统或数据进行访问的功能。  • 禁止隐秘访问方式：包括隐藏帐号、隐藏口令、无鉴权的隐藏模式命令/参数、隐藏组合键访问方式；隐藏的协议/端口/服务；隐藏的生产命令/端口、调测命令/端口；不记录日志的非查询操作等  • 禁止不可管理的认证/访问方式：包括用户不可管理的帐号，人机接口以及可远程访问的机机接口的硬编码口令，不经认证直接访问系统的接口等。 | 满足 | 实测系统内部不存在用户不可管理的账号，人机接口以及可远程访问的机机接口不存在硬编码口令，没有不经认证直接访问系统的接口。 |
| 5.1.1 禁止存在任何“未公开接口”：  2）未文档化的命令/参数、端口等接入方式（包括但不限于产品的生产、调测、维护用途），需通过产品资料等向运营商或监管机构公开或受限公开。 | 满足 | 所有资料都已经向用户公开，不存在其他的接入方式 |

### 访问通道控制

该质量属性标准项描述：系统支持对管理平面的接口的访问保护。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 对于仅支持带外管理的设备，提供管理面隔离的能力，以支持在用户面和控制面使用nmap等工具进行端口扫描都无法扫描到管理平面的地址及端口。 | 满足 | Nmap扫描端口与通信矩阵描述保持一致。 |
| 系统开放的所有端口（不含本地监听端口127.0.0.1）都必需在通信矩阵中有记录；保证通信矩阵中所描述的所有端口都是系统运行和维护所必需的，且描述正确 | 满足 | 通信矩阵描述端口均为系统业务所需。 |
| 通信矩阵中描述的侦听接口范围限定，与实际动态侦听接口范围保持一致。 | 满足 | 动态范围很小，满足要求 |
| 不需要与公网进行交互的产品，默认IPv4地址必须使用“私有地址”。 | 满足 | 系统部件均在公司内网机房内 |
| 所有在设备外部可见的能对系统进行管理的物理接口（如串口、USB接口、管理网口等）应具备接入认证机制，以防止非授权访问. | 满足 |  |
| 所有能对系统进行管理的通信端口及协议必须有接入认证机制，标准协议没有认证机制的除外。 | 满足 |
| 系统的管理平面和近端维护终端（如LMT）、网管维护终端间，支持使用合适的安全协议进行通信。对于不安全协议（如FTP、Telnet），支持关闭。 | 满足 | 不安全协议均关闭 |

### 软件完整性保护

|  |  |  |
| --- | --- | --- |
| **测试要点** | **评估**  **结果** | **说明** |
| 5.1.2 在软件包（含补丁包）发布前，需要经过至少一款防病毒软件扫描，保证防病毒软件不产生告警，特殊情况下对告警作出解释说明。扫描记录（防病毒软件名称、软件版本、病毒库版本、扫描时间、扫描结果等）存档并随软件包（含补丁包）发布给客户。 | 满足 | 使用Symantec、Kav、Avira、OSCE、McAfee扫描，未发现病毒 |
| 5.1.3 基于通用操作系统的软件（包含软件包/补丁包）必须提供完整性校验机制，在安装、升级过程中对软件进行完整性验证。 | 满足 | 已支持了整包完整性校验。使用VMP自带的数字签名机制。 |

### 敏感数据与加密保护

**该质量属性标准项描述：**系统对敏感数据的存储、传输和处理需保证数据安全，并遵从适用国家和地区的法律和法规要求。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 认证凭据不允许明文存储在认证端的系统中，应该加密保护，加密的方式取决于应用场景。对于不需要还原的场景（如用户登录口令），必须使用单向的不可逆算法加密 | 满足 | 1、口令、口令文件、key等在系统中全部为加密存放。  2、不需要还原的场景都是满足要求。 |
| 密钥不允许明文存储在系统中，应该加密保护并提供访问控制。硬编码密钥暂不要求。 | 满足 | 代码检视密钥不会明文存储。 |
| 产品安全敏感数据（如：个人用户使用的口令、操作维护用途的口令、用于网络通信协议协商的身份认证Key等）不得在日志中明文记录。 | 满足 | 1、检查操作日志没有明文敏感数据显示；  2、检查组件DataPush、DataLoad、执行网关相应log不会明文显示敏感数据。 |
| 对敏感数据的访问要有认证、授权或加密机制。 | 不满足 | 部分业务脚本、日志、配置文件权限需按规范设置 |
| 在系统设计时，需识别出产品敏感数据。  口令，银行帐号，批量个人数据等敏感数据如需通过非信任网络传输，产品应支持安全传输通道或者将数据加密后再传输的机制。有标准协议规定除外。 | 满足 | 数据在系统各组件之间传输均有相应加密手段保障数据的安全 |
| 禁止使用私有算法实现加解密 | 满足 | 经安全代码检视，未发现私有加密算法。 |
| 用于敏感数据传输加密的密钥，不能硬编码在代码中，应提供密钥管理或密钥协商的机制。产品CPI资料中应提醒用户修改及定期更新，并提示风险。 | 满足 | 经安全代码检视，未发现硬编码于敏感数据传输加密的密钥 |
| 红线观察项： ·产品中使用的证书应符合以下安全要求： 1）产品应支持按标准格式(如PKCS系列标准)对证书私钥进行保存和加密。使用基于口令的加密机制（如PBES2）时，加密使用的口令需符合口令复杂度要求，并在设备上加密存储； 2）产品禁止提供导出华为预置证书私钥的接口； 3）产品应支持证书替换功能，并在产品资料中提示风险，建议客户替换成自己的证书和公私钥对。 | 不涉及 |  |
| 红线观察项：  ·禁止使用业界已知不安全的加密算法，支持安全的加密算法（标准协议要求或与第三方对接的除外）；  缺省使用安全的加密算法，如客户选择不安全的加密算法，应提示安全风险。 | 满足 | 经安全代码检视，未发现不安全加密算法  使用的AES128CBC加密算法，满足要求。 |

### 日志审计

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 对管理面所有的用户活动都有相应的日志记录。  用户活动包括：  1、登录和注销；  2、增加、删除用户和用户属性（账号、口令等）的变更；  3、用户的锁定和解锁，禁用和恢复；  4、角色权限变更；  5、系统相关安全配置（如安全日志内容配置）的变更；  6、重要资源的变更，如某个重要文件的删除、修改等。 | 满足 | 涉及日志安全中的要求系统存在日志打印 |
| 对管理面所有的操作指令都有相应的日志记录。  操作指令包括：  1、对系统配置参数的修改；  2、对系统进行启动、关闭、重启、暂停、恢复、倒换；  3、对业务的加载、卸载；  4、软件的升级操作，包括远程升级和本地升级；  5、对重要业务数据（特别是与财务相关的数据，包括：卡号、余额、话单、费率、费用、订单、出货、账单等）的创建、删除、修改；  6、所有账户的命令行操作命令。 | 满足 |  |
| 管理面用户活动、操作指令的日志至少包含下列内容：  a. 事件发生的时间；  b. 用户ID(包括关联终端、端口、网络地址或通信设备）；  c. 事件类型；  d. 被访问的资源名称；  e. 事件的结果。 | 满足 |  |
| 1、 产品提供的日志模块/文件有相应的访问控制（如用户名、口令等）  2、 进行日志删除操作必填具备管理员权限。 | 不满足 | 组件日志权限需按规范整改 |

### 操作系统加固与防病毒

**该质量属性标准项描述**：无论是使用通用操作系统（Windows、Linux、Unix等）还是嵌入式操作系统（如VxWorks、pSOS等)，系统都应该保证软件及软件运行环境的安全。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 产品使用Nessus等（使用当时最新的漏洞插件、配置所有插件）进行漏洞扫描测试，产品没有高风险级别漏洞。 | 满足 | Nessus版本为6.3.7，未发现高风险项，有中、低级风险。具体描述见6.2漏洞扫描 |
| 基于通用操作系统的新发货产品“操作系统加固+操作系统补丁”预装率=100%；对于不在生产环节预安装的产品，需要在正式发布的版本中包含默认的安全策略文件，并在产品资料中说明加固要求和操作步骤。 | 满足 |  |
| 新产品发布版本中包含TR5前公司内部发布的最新安全补丁。 | 满足 |  |
| 嵌入式操作系统如存在安全漏洞，产品应制定相应的整改计划，如果无法通过现网安全补丁解决，可落入产品下一个版本。 | 满足 | 检查开源社区，系统内已经存在漏洞均已修复。 |
| 发货时包含Windows操作系统的服务器端产品，产品配置器中缺省配套防病毒软件。 | 不涉及 |  |

### 协议与接口防攻击

**该质量属性标准项描述**：系统应具备基本的防攻击能力，对影响自身的常见攻击具备防御能力等。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 与终端用户有交互、与非信任网络互联、容易受攻击的协议要进行协议畸形报文攻击测试。 | 满足 | 使用Codenomicon扫描标准SSH V2协议。 |

### Web安全

**该质量属性标准项描述：**Web系统必须采取措施降低Web应用安全风险。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| Web应用的认证模块采用防在线暴力破解机制，例如：验证码或者多次连续尝试登录失败后锁定账号/IP。 | 不涉及 | MFS监控web页不存在认证机制 |
| 产品对于每一个需要授权访问的页面或servlet的请求都核实了用户的会话标识是否合法、用户是否被授权执行这个操作。 | 不涉及 | MFS监控web不涉及会话标识等cookie |
| 登录过程中，往服务器端传递用户名和口令时，采用安全协议或加密机制，如HTTPS、HTTP digest等。只提供本地接入、登录，做设备管理使用的场景暂时不要求。 | 不涉及 | MFS监控WEB无登录认证过程 |
| 用户产生的输入必须在服务端进行合法性校验。 | 满足 | 1、存在后台校验 |
| 对用户的最终认证处理过程必须在服务器端进行。 | 不涉及 | MFS监控web不涉及用户认证 |
| 非本Web应用生成的且未经验证的表数据或文件数据在输出到客户端前进行HTML编码，以防止跨站脚本。 | 满足 | 输出至客户端均已经过HTML编码。 |
| 使用Web漏洞扫描工具（如AppScan等工具）对产品Web应用和Web服务器进行扫描测试，扫描结果无高风险级别漏洞，系统无异常。 | 不满足 | 用AppScan扫描有高级别漏洞。开发正分析修改。 |
| 非嵌入式产品的Web应用，应使用预编译语句PreparedStatement代替直接的语句执行Statement，以防止SQL注入。 | 满足 | MFS不涉及数据库相关 |
| 产品的Web应用如果提供上传/下载文件功能，必须在服务器端对文件进行限制（例如：采用白名单方式对上传或下载的文件类型进行限制、对上传或下载的路径进行限制）。 | 满足 | 1、不存在目录遍历。 |

### 产品开发、发布和安装安全

**该质量属性标准项描述：**指产品在开发、发布和安装过程中要保证安全性。

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 产品的C/C++和Java的编码实现应遵循公司安全编程规范中的如下“红线要求”条款（其它安全编程要求请参考公司《C&C++语言安全编程规范》和《Java语言安全编程规范》）。 | 满足 | 危险函数按照编码规范整改 |
| 产品编码完成后，需要经过静态代码检查工具（如Coverity、Fortify）的扫描，并对扫描结果进行分析、处理，确保产品发布时高风险级别及以上问题得到解决。 | 满足 | 具体参考6.7静态扫描分析报告 |

### 数据库加固

BI大数据平台BI DSPT 1.0.3.100版本不涉数据库组件。

### 口令安全

|  |  |  |
| --- | --- | --- |
| **测试检查项** | **评估**  **结果** | **说明** |
| 对于人机接口或可远程访问的机机接口之间，产品默认在所有口令设置时进行复杂度检查，若口令不符合复杂度规则，必须禁止设置并进行警告。（口令复杂度要求见“口令安全要求”）如果产品支持用户关闭复杂度检查机制，应在CPI资料中提示风险。 | 满足 |  |
| 对于人机接口或可远程访问的机机接口之间，产品提供防暴力破解机制如登录失败尝试次数超阈值时的锁定（帐号或IP等）和解锁机制。对于只能在物理上本地操作的接入认证（如进入BIOS），不强制提供锁定机制 | 满足 | 1、存在多次登录失败锁定账号 |
| 对于系统自身操作维护类的口令，输入口令时口令不能明文回显，命令行参数输入的场景不作要求。 | 不涉及 | 1、不涉及口令明文回显的场景 |
| 系统提供的口令输入框不支持口令拷出。 | 不涉及 |  |
| 系统帐号的缺省口令（如操作系统、数据库、业务系统），口令应符合复杂度的要求。 | 不满足 | 服务器认证密码复杂度需按要求整改 |
| 用户修改口令前需再次验证旧口令。  管理员重置其他用户的口令，无需验证旧口令。 | 不涉及 |  |
| 用户仅可以修改自身帐号的口令，管理员除外。 | 不涉及 |  |
| 在数据库、配置文件、日志、cookie、调试跟踪信息中不得存储口令的明文。 | 满足 | 在配置文件、日志、cookie、调试跟踪信息中不得存储口令的明文 |
| 如系统支持文件访问控制，口令文件必须设置访问权限，普通用户不能读取或拷贝加密的内容。 | 满足 |  |
| 产品CPI资料中需描述系统的默认帐号和口令,提醒用户修改默认帐号/口令及定期更新，并提示风险。 | 满足 |  |

## 安全设计改进建议

设计时可以考虑整体的安全性，包含接口、操作系统、日志等场景，确保交付立体安全。

# 产品安全性问题/风险汇总和跟踪

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **产品安全性问题/风险描述** | **质量风险等级** | **改进建议** | **结论跟踪** |
| 1 | AppScan扫描高风险问题1个 | 无 | 按要求整改 | 开发正分析修改并同步备案 |
| 2 | 测试环境文件权限问题2个 | 低 | 按规范配置环境脚本、日志等文件权限 |  |
| 3 | 服务器认证密码复杂度问题1个 | 低 | 按密码复杂度要求配置整改 | 已按要求整改 |
| 4 | 业务进程启动用户问题1个 | 低 | 按要求整改为业务用户启动 | 已整改为非root用户 |
| 5 | 日志删除自动生成问题1个 | 低 | 后续版本解决 |  |

本次安全测试内容包括安全需求验收、安全红线测试、端口扫描/漏洞测试、协议健壮性测试、攻击测试等几个方面。发现问题及DTS单号如下：

* + - 1. DTS2016042905061 【Appscan扫描】MFS组件自身提供的web监控页面存在跨站脚本注入点
      2. DTS2016042904595 待测组件业务进程为root启动
      3. DTS2016042904433 待测组件服务器身份认证密码复杂度不够
      4. DTS2016042904268 待测组件相关日志文件权限未严格设置，非业务相关用户可读取业务日志
      5. DTS2016042904161 待测组件相关脚本及配置文件权限未严格设置
      6. DTS2016042902147日志文件删除后的自动生成异常

目前遗留1个严重问题和3个提示问题，其中1个严重问题（AppScan问题）开发正在分析修改并同步走备案流程，2个服务器脚本、日志、配置文件等权限问题待按照规范整改，1个日志删除自动生成问题作遗留问题后续版本解决。

**测试问题分析总结：**在已发现问题中，敏感数据保护、Web安全、编码安全、日志安全、口令安全等重点风险项。在后续版本中，测试改进：

(1) 提升功能测试团队网络安全意识，将日志测试融入到功能测试中，保证日志审计测试完全性；

(2) 口令测试除了现有黑盒测试外，针对口令编码也要有针对性的进行代码检查，防止口令硬编码；

(3) 敏感数据保护，需要做到白盒检视和黑盒验证，每轮迭代扫描，重点关注配置和日志打印。

(4) 提高检视代码和扫描结果效率，多从白盒角度发现代码潜在的安全风险；

(5) 口令安全严格按照口令安全，检查提示、加密、打印的方面关注其安全性。

# 测试结论

BI大数据平台BI DSPT 1.0.3.100版本主要全量覆盖《云业务安全测试基线用例集V1.1》进行测试。

该版本经排查，产品发现安全问题均已按计划修改，遗留部分问题已经单独澄清， APPSCAN中风险问题有风险分析及解决计划，Fuzz（Codenomicon）SSH V2协议测试通过，未发现问题。

已经达到《BI大数据平台安全测试策略V3.0》中SDV&SIT网络安全测试出口条件。

# 附件

## 端口扫描结果

Nmap端口扫描原始报告：



## 安全漏洞扫描结果

漏洞扫描原始报告：



## Web系统漏洞扫描结果

AppScan扫描原始报告：

**

## Codenomicon Defensics扫描结果

Codenomicon Defensics扫描报告：



## 防毒软件扫描结果

（不涉及）

## 安全红线自检报告及举证材料

**

## 源代码静态安全扫描分析报告



## 通信矩阵

