|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | |  |
|  | | |
|  | | |
| 方圆ok1 | | | |
|  | BI数据平台安全技术白皮书 | | 附件1-16K |
|  | |
|  |  |
| **发布日期** | 20160427 |
|  | |
| 华为技术有限公司 | |
|  | | |

目 录

[1 终端云业务安全概述 2](#_Toc365397576)

[2 网络安全 4](#_Toc365397577)

[3 系统安全 5](#_Toc365397578)

[4 应用安全 6](#_Toc365397579)

[5 数据安全 7](#_Toc365397580)

[6 总结 8](#_Toc365397581)

[7 缩略语 9](#_Toc365397582)

# 消费者云服务业务安全概述

随着电信网络和信息技术的不断演进与发展，网络安全面临的威胁和挑战将日益严重。华为对此高度重视，并致力于采取切实有效的措施提升产品和服务的安全性，从而帮助客户规避和减少安全方面的风险，以赢得各利益相关者的信赖。华为认为，构建一个开放、透明、可视的安全问题解决框架，将有助于整个产业链持续健康发展，同时也承诺将构筑并全面实施端到端的全球网络安全保障体系作为公司的重要发展战略之一，在遵从所有适用的国家和地区安全法规、国际电信标准和参考行业最佳实践的基础上，从政策、组织、流程、管理、技术和规范等方面建立和完善可持续、可信赖的安全保障体系，并与有关政府、客户及行业伙伴以开放和透明的方式，共同应对安全方面的挑战，全面满足客户的网络安全需求。

使用智能终端设备的用户越来越多，基于智能终端开发的移动互联网业务（在本文统称“终端云业务”）逐步融入人们的日常生活，在为用户提供便利的同时，终端云业务安全也越来越被用户关注。终端云业务安全面临的主要问题和威胁分类如下：

* + - * + **网络安全威胁：**数据拦截或篡改、不安全传输协议、密钥泄露等；
        + **系统安全威胁：**操作系统的漏洞、操作系统的不当配置等；
        + **应用安全威胁：**病毒、木马、流氓/恶意软件、黑客针对性攻击等；
        + **用户数据安全威胁：**用户隐私泄露、数据丢失、账号密码窃取、窃听等。

华为持续致力于终端云业务的安全性研究和开发，努力打造安全、可靠的终端云业务系统。华为将终端云业务安全通过如下几个层次进行描述：

|  |
| --- |
| **网络安全** |
| **系统安全** |
| **应用安全** |
| **数据安全** |

# 网络安全

BI数据平台的所有业务仅对华为内部员工、内部业务部件提供服务。业务在网络中传输重要、敏感数据时，采用安全传输通道同时针对个人敏感数据进行加密传输来保证数据的安全，另外，在网络入口处部署安全设备，例如：防火墙、入侵（检测）防御系统、ip白名单控制等保护业务系统安全，为用户提供安全可靠的业务系统。

**VPN**

BI数据平台提供的面向最终用户的服务，要求必须接入公司iaccess或运维vpn才可以进行相关的业务操作。

**SSL/TLS**

所有面向用户的服务均采用SSL安全传输协议。支持SSL v3和TLS v1.0/1.1/1.2。

**防火墙**

只开放业务必须使用的端口供用户访问，并对进出业务系统网络的数据包进行过滤，避免业务系统受到网络层攻击。

**入侵（检测）防御系统**

业务部件之间的交互采用ip白名单进行控制，内部部件采用内部ip通信，外部部件进行证书验证。

# 系统安全

本章节主要关注OS的系统安全及安全策略等。华为密切与操作系统厂商合作，跟踪操作系统的漏洞的发布，及时升级系统的补丁；同时也关注操作系统的安全策略的配置，保证系统的权限进行合理的分配、多余的服务和协议端口会被关闭以及系统的账户被合理的管理等。

**系统安全**

通过镜像签名认证机制保证设备系统的完整性，确保系统不会被非法篡改。华为与业界主流OS厂商保持密切的合作关系，有专门的组织和人员跟踪主流OS的漏洞和补丁发布，密切跟踪各OS平台的安全漏洞发布情况。在研发中会使用业界知名的系统漏洞扫描工具对系统进行漏洞扫描，并对操作系统存在的安全风险进行及时修复。

**系统安全策略**

在终端云业务开发中对于需要使用的端口以及服务会进行审视，如存在安全风险或非业务必须，在业务部署时会将没有使用的服务或端口进行关闭、没有使用的账户被删除，同时确保系统的安全功能不会被关闭，并从安全的角度对于系统默认配置进行审视。

# 应用安全

华为终端云业务提供了丰富的业务满足人们不同的业务需求，适合在不同场合的使用，如通过手机、平板电脑、家庭电脑等访问使用。华为终端云业务在开发、测试、发布、维护等各个阶段都有严格安全规范和审查流程，积极利用各种有效的安全技术和管理手段来保证业务的安全性。

BI数据平台是终端云业务之一，符合终端云业务安全的各流程和要求。同时在访问控制上做出了更高的要求，普通用户必须接入公司iaccess才能访问，运维用户通过运维vpn接入后访问。

**开发安全**

开发过程中要遵循安全编码规范，同时采用业界主流代码扫描工具对产品代码进行扫描确保codecc全部清0，减少安全漏洞的存在。

**应用测试安全**

按照公司的安全测试规范及安全能力中心要求规范等要求进行安全测试。包括但不限于 根据不同的使用场景进行一系列相关的安全测试，减少安全漏洞的存在，防止给用户造成不必要的损失。安全测试包括病毒木马、端口、漏洞、Web安全等扫描、协议攻击测试等。

**发布安全**

服务器部件，仅服务公司内部人员，有专人负责部署到公司专用机房。不涉及客户端，不涉及版本对外发布。

**敏感数据保护**

所有涉及的用户个人数据、敏感数据。无论在运算还是传输过程中都按照公司规范进行加密。同时传输时使用SSL安全通道。

**第三方应用安全**

对于开源代码的使用，除了遵循其开源协议外，也会对其进行严格的安全审查(如代码安全扫描、漏洞扫描等)，对存在的安全漏洞加以修复。同时定期与其开源社区保持联系，及时更新补丁，以保证产品的安全性。

# 数据安全

为了保证数据的安全，防止数据被非法访问或破坏，华为终端云业务采用了多种技术手段，包括安全算法、数据的安全存储及访问、备份恢复、内容保护等。华为充分尊重用户的隐私和通信自由，尊重当地的法律法规，对于个人数据的使用及处理有明确的隐私政策声明。

**安全算法**

采用国际标准或业界通用的安全算法(如3DES、AES、RSA、ECC、DSA、RC4等)，对于密钥、证书、授权认证的管理也有严格的流程。

**数据安全存储及访问**

* + - * + **权限控制：**对不同的用户分配不同的权限以限制对数据的访问；
        + **数据加密：**通过对数据加密防止非法访问。

**数据的备份及恢复**

华为终端云业务会定期对数据进行备份，并对备份数据进行合理保护。一旦有需要能够及时进行数据恢复，保证用户正常的业务使用。

**隐私政策**

华为始终坚持以客户为中心，高度重视保护用户的个人隐私和数据。在经过用户允许的情况下华为终端云业务可能会收集一些个人信息，对于个人信息的处理会提供加密或匿名化等安全措施进行处理，确保个人数据安全，收集的数据仅用于用户所要求提供的服务或提升产品的体验，包括最新产品资讯、软件升级、服务等。在涉及个人隐私信息的产品中会附有华为公开的隐私政策声明，关于华为隐私政策详细信息参考：<http://consumer.huawei.com/cn/privacy-policy/index.htm>

# 总结

华为致力于提供业界最好的产品和服务以满足客户的需求。我们非常重视网络安全，已经投入了很多资源去提升和改善我们公司、业界同行以及其他各方的能力，为产品提供安全保障。

华为在内部还建立了独立的网络安全实验室及安全测试团队，对产品进行网络安全专项测试；同时华为积极、持续地参与ITU-T、3GPP、IETF等国际电信标准组织中的安全标准制定，加入FIRST（应急事件及安全团队论坛）等安全组织，并通过和主流安全厂商紧密合作，为行业的健康发展作出自己的贡献，努力保障全球客户的网络安全。

华为成立了监控、受理产品安全漏洞的专门组织PSIRT（产品安全事件应急响应团队），华为希望安全研究人员、行业组织、政府组织和供应商主动与华为PSIRT联系，报告潜在的华为产品的安全漏洞或安全问题。

华为PSIRT E-mail邮箱：[PSIRT@huawei.com](mailto:PSIRT@huawei.com)

注：1. 华为面向全球发布了网络安全白皮书——《网络安全透视： 21世纪的技术与安全—一场艰难的联姻》。该白皮书由华为全球网络安全官约翰.萨福克（John Suffolk） 撰写，详细参见如下链接：

中文：<http://www.huawei.com/ilink/cn/download/HW_187369>

Eng：<http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_187368.pdf>`

2.关于华为PSIRT的详细说明请查看如下链接：

中文：<http://www.huawei.com/ilink/cn/special-release/HW_093772>

Eng：<http://www.huawei.com/ilink/en/special-release/HW_093771>

# 缩略语

|  |  |  |
| --- | --- | --- |
| 英文缩写 | 英文全称 | 中文全称 |
| 3DES | Triple Data Encryption Algorithm | 数据加密算法 |
| 3GPP | The 3rd Generation Partnership Project | 第三代合作伙伴计划 |
| AES | Advanced Encryption Standard | 高级加密标准 |
| API | Application Programming Interface | 应用软件编程接口 |
| CA | Conditional Access | 条件接收 |
| Cloud+ | Cloud+ | 华为终端提供的云业务 |
| DSA | Digital Signature Algorithm | 数字签名算法 |
| EAP | Extensible Authentication Protocol | 扩展认证协议 |
| ECC | Elliptic Curves Cryptography， | 椭圆曲线密码编码 |
| FIRST | Forum of Incident Response and Security Teams | 应急事件及安全团队论坛 |
| IETF | Internet Engineering Task Force | 互联网工程任务组 |
| IPSec | IP Security | 因特网协议安全协议 |
| ITU-T | International Telecommunications Union Telecommunication Standardization Sector | 国际电信联盟远程通信标准化组织 |
| L2TP | Layer 2 Tunneling Protocol | 2层隧道协议 |
| OS | Operating System | 操作系统 |
| PSIRT | Product Cyber Incident Response Team | 产品安全事件应急响应团队 |
| PSK | Phase Shift Keying | 相移键控 |
| RC4 | Rivest Cipher 4 Algorithm | RC4加密算法 |
| RSA | RSA Algorithm | 公开密钥密码体制 |
| SSL | Security Socket Layer | 加密套接字协议层 |
| TLS | Transport Layer Security | 传输层安全 |
| VPN | Virtual Private Network | 虚拟专用网 |