**华为技术有限公司**
深圳龙岗区坂田华为基地
电话：+86 755 28780808
邮编：518129
www.huawei.com

# 华为漏洞管理白皮书

**商标声明**

HUAWEI, HUAWEI, 是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

**免责声明**

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

**版权所有© 华为技术有限公司2023。保留一切权利。**

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

华为漏洞管理白皮书

# 目录


1 前言 ····· 03

2 漏洞管理是保障网络空间安全的重要工作 ····· 03

3 漏洞管理是产业链的共同责任，需要协同合作来共同解决 ····· 03

4 华为遵循行业标准和最佳实践建立漏洞管理体系和工程能力 ····· 04

4.1 华为漏洞管理理念 ····· 04

4.1.1 漏洞管理目标 ····· 05

4.1.2 漏洞管理原则 ····· 05

4.1.3 漏洞处置关键阶段 ····· 05

4.1.4 漏洞管理行为准则 ····· 06

4.2 华为漏洞管理框架与实践 ····· 07

4.2.1 全量漏洞管理 ····· 07

4.2.2 全生命周期漏洞管理 ····· 08

4.2.3 全供应链管理 ····· 09

4.2.4 漏洞管理平台 ····· 09

5 总结 ····· 10

# 1 前言

随着大数据、工业互联网、云计算以及人工智能等技术的快速发展和应用，一方面，新技术促进了企业数字化业务的进程，带来了数字经济繁荣;另一方面，新技术也使得软件架构日益复杂化和新攻击手段的涌现，导致企业业务系统暴露出更多的安全漏洞。

在网络安全事件频发的大背景下，企业对网络安全风险意识不断增强，漏洞管理被越来越多的企业所重视并成为企业网络安全战略的重要组成部分。同时，各国家和地区通过立法对网络安全漏洞进行统筹风险管理。

# 2 漏洞管理是保障网络空间安全的重要工作

近年来，网络空间安全威胁不断升级，网络勒索、供应链安全等事件频发，造成严重损失，漏洞仍然是安全事件的主要触发点之一。围绕产品全生命周期构筑全供应链的端到端漏洞管理，是降低现网风险、保障业务连续运行的重要手段。

随着全球产业数字化转型的深入，网络安全攻击向常态化、自动化发展，高风险漏洞和安全事件成为立法监管和相关技术孵化的加速剂，中英欧美等国陆续发布相关法规统筹漏洞管理，漏洞管理已成为国家网络安全战略的重要部分。

漏洞管理的成熟度是企业数字化治理水平和软件工程能力的直接体现，与企业可持续发展密切相关，企业要和各利益方持续协同管理漏洞，否则可能面临系统瘫痪、信息泄露等风险，损害企业资产和声誉，甚至影响企业的长远发展。

# 3漏洞管理是产业链的共同责任，需要协同合作来共同解决

漏洞管理涉及端到端供应链，如供应商（包括开源社区）、设备商、运营商、最终消费者等多个利益相关方，也涉及产业全生命周期的漏洞感知、验证、修补、披露、现网漏洞风险消减等多个环节，如何确保漏洞信息在各利益相关方的及时、准确、安全的交互是行业挑战。同时企业内部产品、平台、组件等现代软件大规模的多组织协同开发，进一步加剧了漏洞管理的复杂性。

漏洞管理需要供应链上下游协同，促进各责任方履责，以开放合作的态度，在供应链上下游构筑持续信赖的合作关系，不断提升信任与能力，共同消减漏洞带来的网络安全风险。





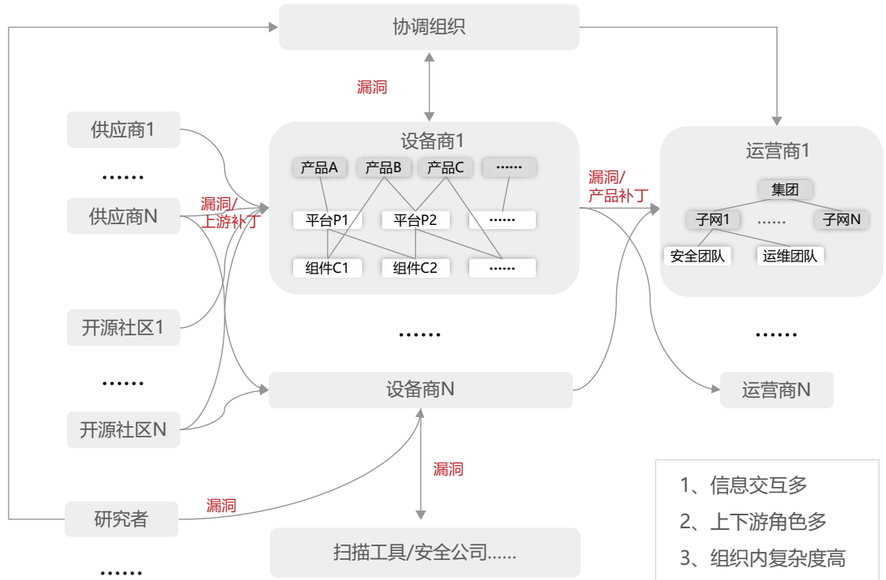


图3−1 漏洞管理的协同/协作关系图

# 4 华为遵循行业标准和最佳实践建立漏洞管理体系和工程能力

## 4.1华为漏洞管理理念

华为将“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，从政策、组织、流程、技术和规范多方面建立可持续、可信赖的漏洞管理体系，与外部利益相关方开放协同，共同应对漏洞的挑战。华为对漏洞管理提出五项基本原则，确定七个漏洞处置阶段和相应的行为准则，指导业务部门开展漏洞管理活动。

图4− 1 漏洞管理理念架构

### 4.1.1 漏洞管理目标

为了更好的支撑客户现网漏洞风险消减，华为将漏洞管理的目标具体分解成以下三个主要方面：

1、负责任披露：对购买华为产品和解决方案的客户，建立漏洞披露与沟通机制，支撑客户对漏洞风险决策。

2、减少和消减漏洞：建立全量、全生命周期、端到端漏洞管理机制，实现漏洞及时感知、排查、规避和修补，支持客户风险消减。

3、协同管理：明确与供应商和客户的漏洞管理协同机制，共同协作消减漏洞风险。

### 4.1.2 漏洞管理原则

1、减少伤害和降低风险

减少或消除漏洞给客户带来的伤害，降低华为产品、服务的潜在风险，既是漏洞管理的愿景，也是漏洞处置&漏洞披露时所遵循的价值指引。

2、减少和消减漏洞

漏洞不可避免是业界已经形成的共识[1][2][3]，但我们一直在努力：1）采取措施减少产品和服务中的漏洞；2）一旦发现产品和服务中的漏洞，及时向客户/用户提供风险消减方案。

3、主动管理

漏洞问题需要供应链上下游协同合作来解决，我们会主动先厘清边界再履行责任，基于法规、合同和公开标准要求等，构建漏洞管理体系主动开展漏洞管理。

4、持续优化

网络安全是持续演进的动态过程，威胁和攻击在更新，防守也要持续更迭。我们将持续优化，不断借鉴行业标准和业界优秀实践，提升漏洞管理的成熟度。

5、开放协同

我们将秉持开放合作的态度，加强供应链和外部安全生态的联接，并加强与利益相关方的协同，构筑可信赖的合作关系。

### 4.1.3 漏洞处置关键阶段

华为致力于提升产品和解决方案的安全性，全面支撑客户网络和业务的安全运营。参考ISO/IEC 30111、ISO/IEC 29147标准建立完整的漏洞处置流程，持续为产品安全性保驾护航，并建立开放协同生态，共同应对漏洞风险挑战。

[1] https://www.tenable.com/blog/vulnerabilities-in-cybersecurity-how-to-reduce-your-risk

[2] https://www.ntia.gov/files/ntia/je_savage_05182015.pdf

[3] https://www.secpoint.com/vulnerabilities-are-unavoidable.html





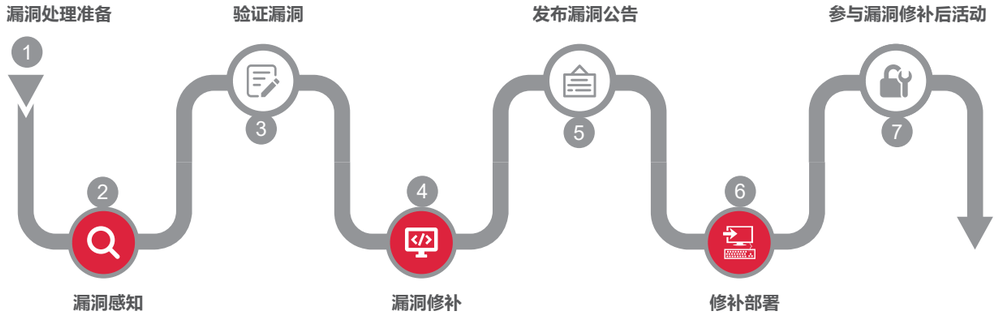


图4-2 漏洞处置的7个关键阶段

1、漏洞处理准备：构建漏洞披露和处理的策略、组织和能力；
2、漏洞感知：建立漏洞感知渠道，接收相关疑似漏洞；
3、验证漏洞：确认疑似漏洞的有效性和影响范围；
4、漏洞修补：制定并落实漏洞修补方案；
5、发布漏洞公告：面向客户发布漏洞修补信息公告；
6、修复部署：运营者收到漏洞修补信息后，评估风险并现网部署，消减风险；
7、参与漏洞修补后活动：结合客户意见和内部实践持续改进。

### 4.1.4 漏洞管理行为准则

为了更好地指导各业务部门开展漏洞管理活动，针对漏洞处置过程的关键活动，提出漏洞管理行为准则：

在漏洞处理准备阶段，需建立漏洞处理的组织与流程，明确漏洞处置目标，并与外部建立沟通渠道。

在漏洞感知阶段，应建立广泛的内外部漏洞感知渠道，全面感知与华为产品相关的漏洞信息，以便及时对漏洞进行验证和修补。

在验证漏洞阶段，验证感知到的漏洞对生命周期内版本的影响情况，在此期间保持与漏洞上报者持续、清晰的沟通。

在漏洞修补阶段，应积极采取行动对漏洞进行修补&消减。同时基于漏洞严重等级，对漏洞进行分级的响应，确保所有漏洞都得到合理处置。

在发布漏洞公告阶段，需遵循受影响告知的原则，即漏洞信息仅披露给受影响的利益相关方，同时做好内外部协同。

在修复部署阶段，在支撑客户或自身修复部署时，开展高风险漏洞的主动沟通，倡议客户/用户积极开展补丁管理建设，鼓励客户/用户主动关注安全更新公告，及时感知并消减。

在参与漏洞修补后活动阶段，产品团队应开展漏洞的根因分析来改进安全活动。另外通过外部沟通、产业链上下游的协同，持续发展和培养全员安全意识与能力。

## 4.2 华为漏洞管理框架与实践

围绕支撑客户现网漏洞风险消减的管理目标，华为建立漏洞管理框架，包括政策、流程、工程、文化与组织，并持续优化各领域能力，支撑漏洞管理的高效、有序开展。

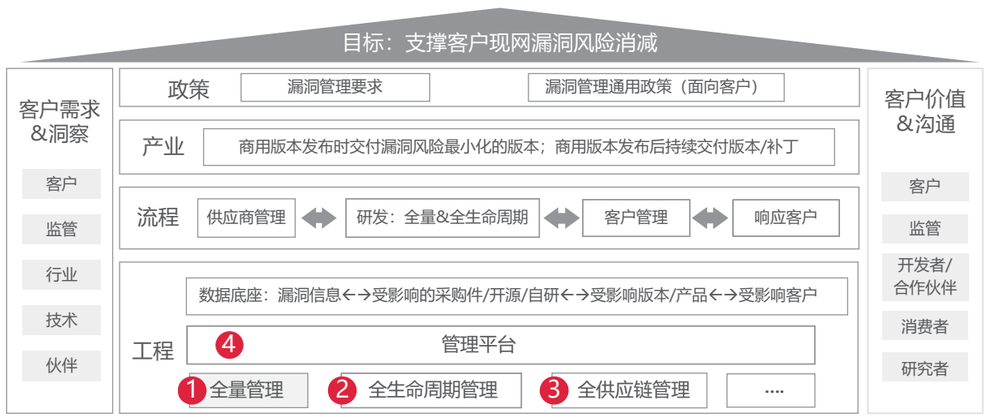


图4-3 华为漏洞管理框架

### 4.2.1 全量漏洞管理

资产管理是漏洞管理的基础，如何确保资产信息的完整性和准确性是行业挑战。华为产品涉及多个产业，拥有ICT、云服务、终端、车等诸多不同类型的产业资产，获取全面且更新的资产清单是个挑战，识别资产中准确的开源软件、三方件等成分也同样是业界难题。

华为明确产业商业领袖作为漏洞管理的第一责任人。在产品立项时，须进行资产注册，从源头确保资产清单纳入管理；在开发过程中，通过软件工程能力（全量源码构建等）确保使用的资产来源已源头纳管，包含使用的平台、开源软件、三方件等。

基于获得的全量软件资产，形成产品版本的全量漏洞视图，在此基础上开展验证、修补等漏洞管理相关的业务活动。

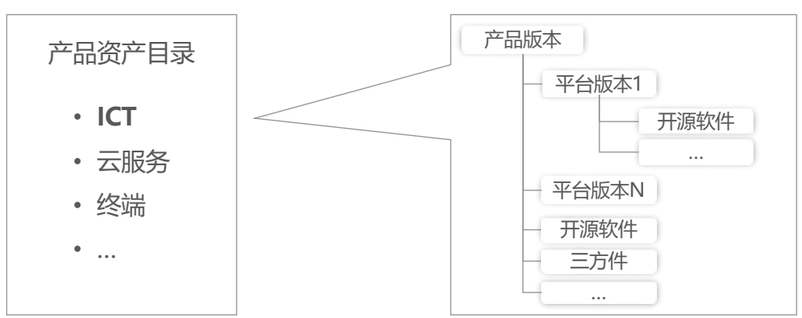


图4-4 全量管理示意图





### 4.2.2 全生命周期漏洞管理

华为将“在设计中构筑安全、在流程中构筑安全、在运作中构筑安全”的理念贯穿在产品的全生命周期，通过流程确保网络安全保障措施在各阶段有效落地，提升产品的安全竞争力。

图4-5 网络安全Built-in IPD流程

“集成产品开发流程”（IPD, Integrated Product Development），从概念、计划、开发、验证和发布阶段，将威胁建模、安全设计、安全开发、安全测试等Build-in流程中，从机制上减少漏洞的引入，在版本发布时，向客户交付漏洞风险最小化的产品版本。

漏洞管理基于产品/软件版本的生命周期里程碑进行管理，华为对停止服务与支持（EOS）前所有产品版本的漏洞进行管理，根据不同生命周期阶段修补策略，在停止全面支持（EOFS）前发布漏洞修补方案（包括缓解措施、补丁/版本等），支持客户例行消减现网漏洞风险。

华为漏洞管理中心持续识别公众广泛关注且已活跃被利用的“高风险”漏洞，并加快漏洞响应的过程，在24小时内发布SN（Security Notice，安全公告）向受影响的客户通知。当有漏洞修补方案后，华为会通过SA（Security Advisory，安全通告）为相关受影响客户提供风险决策和消减支持。

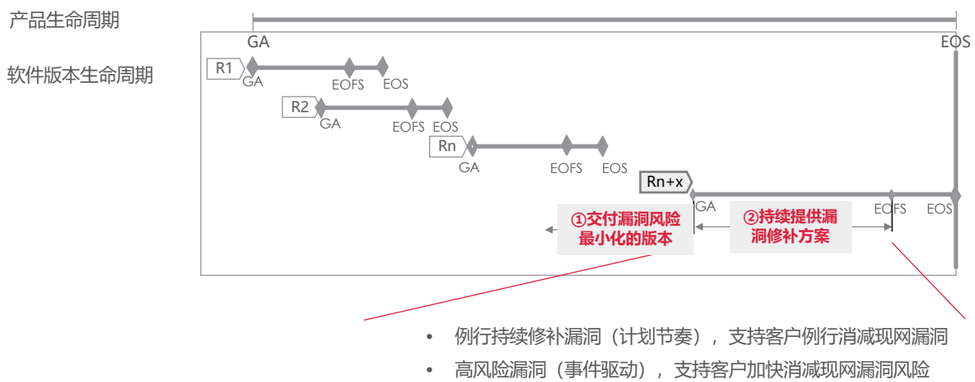


图4-6 全生命周期内漏洞管理示意图

### 4.2.3 全供应链管理

华为拥有复杂的产品、服务与解决方案组合，服务于全供应链中不同类型的客户，承担了包括供应商、设备商/集成商和运营者等在内的多个角色，角色的多样使得华为有机会站从不同视角认识到供应链管理协同的重要性。

图4-7 供应链上下游角色示意图

作为供应商，建立漏洞接收和感知渠道，以保证漏洞的及时、准确感知。同时，面向下游设备商/集成商，建立漏洞披露网站和主动沟通的渠道，通过持续提供漏洞修补方案，支持下游设备商/集成商对修补方案的集成和发布。

作为设备商/集成商，同供应商建立漏洞接收、披露、协同与响应机制。同时，开展漏洞奖励计划项目，鼓励安全研究者、组织等上报产品疑似漏洞。面向客户，建立漏洞披露网站和主动沟通的渠道，以SA/SN、RN（Release　Notes）的方式，向客户进行漏洞披露，支持客户知情决策和现网漏洞风险消减。

作为运营者，同设备商/服务提供者建立漏洞接收、披露、协同与响应机制。在现网资产管理基础上，持续开展漏洞感知、评估和现网修复等活动，将现网漏洞风险控制在可接受的水平。

### 4.2.4 漏洞管理平台

华为ICT、终端、IAS等不同产业承担的角色不同，责任也不相同。为了保障各个产业履责，支撑客户漏洞风险消减，华为漏洞管理中心作为漏洞信息和组织的汇聚点，建立集团统一的管理平台，通过原始作业活动获取数据，形成各产业漏洞管理水平和履责状态的“画像”，实现对全产业漏洞管理结果的“可视”、“可管”。

尊重不同产业行业特点的差异，引导产业持续自我改进和优化，为客户提供更高效、更专业的漏洞管理支持。





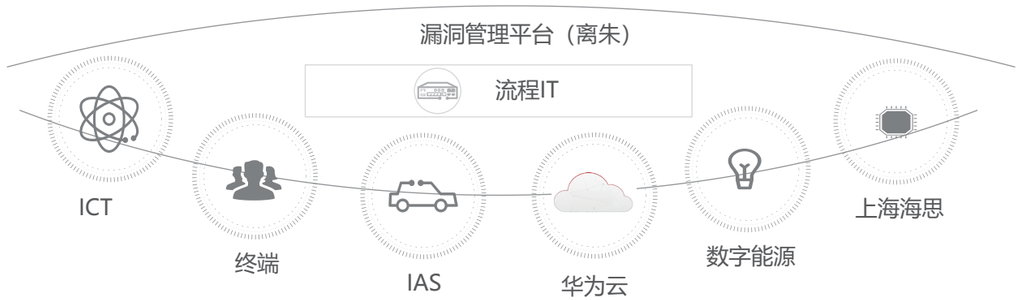


图4-8 漏洞管理平台示意图

## 5 总结

华为充分认识到漏洞管理对数字空间安全的重要性，在漏洞管理五项基本原则的指导下，以消减客户现网风险为目标，通过遵循行业标准和最佳实践开展漏洞管理相关活动，已建立全量、全生命周期的和全供应链为核心能力的端到端漏洞管理体系。

新技术以及新的威胁总是在不断演进和更迭，漏洞管理需要持续迭代和优化。华为愿意分享我们的经验和实践，与客户和伙伴构筑协同、信任的生态环境，携手迎接漏洞带来的网络安全风险挑战。