**国家标准《信息安全技术 路由器安全技术要求》**

**修订说明**

1. 工作简况

1.1 任务来源

2014年12月中央网信办网络安全协调局正式下达国家标准“信息安全技术 路由器安全技术要求”修订任务书。负责人: 卿斯汉。

国家标准《信息安全技术 路由器安全技术要求》的修订工作由中国科学院软件研究所牵头，华为技术有限公司和新华三技术有限公司共同参与修订。

随着工作任务的展开，迈普通信技术股份有限公司、中国科学院信息工程研究所信息安全国家重点实验室和北京大学软件与微电子学院加入了标准修订的队伍。

1.2 主要工作过程

 **1. 2015年1月建立标准修订组，进行广泛调研**

2015年1月标准修订组成立后，随即展开广泛调研，摸清国内外的研究动向，为本标准的制定夯实牢固的基础。在国内外调研中，首先对面临的安全问题进行了概括：

* 网络设备间通信

与其它网络设备或实体间的通信会穿过其它各种各样的系统，中间系统可能是不可信的，这样就存在对网络设备非授权访问、或威胁到合法连接的安全。

— 非授权的管理访问

攻击者可能试图通过恶意方式，获取对网络设备的管理员访问权限。

— 弱加密

如果对加密算法、模式、密钥强度的选择不当，攻击者就有机会进行强力破解，未经授权而获得对设备的操作和控制访问权。

— 不可信的通信通道

不使用非标准的安全协议。由于非标准的安全协议没有经过严格的评估、检验，在设计上可能存在缺陷。攻击者可能通过中间人攻击、替换攻击等方式，使设备受到威胁。

— 弱端点验证

* 更新时可能产生安全问题
* 审计

保证设备审计信息的安全很重要。审计信息的存储、传输过程中需要防止未经授权的删除和修改。

* 管理员和设备的凭证和数据

网络设备上都包含秘密信息，这些秘密信息和凭证需要安全地存储，只有授权的实体才能访问。

* 设备失效

在启动或在运行期间，网络设备的元件可能会失效，使安全功能受到威胁或失效。

* 信息泄露

受保护网络中的设备（内部设备）可能会受到外部设备的威胁，外部设备可能会执行非授权活动。如果外部恶意设备能够和受保护网络中的设备进行通讯，或内部设备和外部设备建立通讯连接，则内部设备可能会受到影响，泄露信息。

* 对服务不恰当的访问

对于进入和外出的连接，都要进行安全的配置。

* 对服务的滥用和误用

当被保护网络外部的设备被允许访问受保护网络内部提供的公共服务时，外部设备可能试图执行恶意行为。当从受保护网络进行外部访问时，该服务可能会存在风险。

* 保障数据完整性

一个受保护的网络中的设备可能会暴露在受保护网络外部的设备的威胁之下，它们们可能试图在未经授权的情况下修改数据。如果已知的恶意外部设备能够和受保护网络的设备进行通讯，或者，如果受保护网络中的设备与外部设备间可建立通讯，则通讯中包含的数据会受到影响，丧失其完整性。

* 防止重放攻击

面对这些安全威胁，在安全功能需求方面应当在标准修订中有所体现。

关于国内路由器的实际应用，我们对常用密码算法的使用进行了调研，结果发现存在大量使用国外密码算法的情况：

* 密码算法：通常支持AES128位及以上或更高强度的密码算法
* 密钥管理

— 私钥的产生

设备通常支持以下类型和强度的密钥（不少于2种）：RSA 2048-bit及以上；ECDSA P256及以上；DSA 2048-bit及以上；DH 2048-bit及以上

— 密钥协商

设备通常支持如下密钥协商算法（不少于2种）：基于RSA的密钥协商； 基于椭圆曲线的ECDH密钥协商；基于有限域的DH密钥协商。

 有鉴于此，有的专家建议本标准修订时可考虑我国实践，支持国外密码算法的使用。但这样就违反了国家相关政策，因此该建议未被采纳。

 **2. 工作组4次内部讨论**

从2015年3月1日至2016年8月31日，工作组内部共进行了4次内部工作讨论，分别提出了修订原则和修订内容，并对提出的修改意见进行反复讨论和推敲。最重要的共识是：不能在本标准中支持国外密码算法。最终形成标准草案版本v.1.0。

 **3. 2016年2月19-20日召开工作组全体会议**

2016年2月19-20日，在北京蟹岛会议楼，召开了工作组全体会议，各标准修订单位（中国科学院软件研究所、华为技术有限公司、杭州华三通信技术有限公司和迈普通信技术股份有限公司）的负责人与专家参加了会议。对标准修订草案v.1.0进行了深入讨论。最后，确定了下一步计划和具体分工，在9月1日前形成标准草案版本v.2.0。

 **4. 2017年6月13-22日工作组内部讨论**

2017年6月13日至2017年6月22日，工作组内部进行了内部讨论，对标准草案版本v.2.0进行了修改，重点研究标准中是否应当包含近期出现的一些新的复杂攻击方法及其防护措施。最终形成标准草案版本v.3.0。

 **5. 2017年6月26日WG5组织专家评审**

2017年6月26日，WG5组织专家评审，地点：中国科学院信息工程研究所3224会议室。到会专家共7人：WG5副组长李嵩，崔书昆，肖京华，许玉娜，陈冠直，李健，刘楠，对标准草案版本v.3.0进行了评审，提出了宝贵建议。在此基础上，工作组做了进一步修改，最终形成标准草案版本v.4.0。

 **6. 2017年7月25-26日WG5工作组全体会议，形成标准征求意见稿**

2017年7月25-26日，在北京远望楼召开了WG5工作组全体会议，卿斯汉代表标准修订组做了标准修订工作报告及标准草案版本v.4.0，以及意见汇总和反馈的说明。本次会议同意本标准进入“征求意见稿”阶段。2017年8月10日，经标准修订组参考反馈意见后形成标准（征求意见稿）版本v1.0。

1. 修订原则和主要内容

2.1 修订原则

《路由器安全技术要求》通过借鉴国外标准的研究，结合新的技术发展和国内应用实践，提出与国际标准接轨、适合我国国情，具有可操作性的“路由器安全技术要求”标准。通过该标准的实施，确保路由器应用及其本身的安全。为路由器产品安全的设计和实现，保障网络安全提供指导。

《路由器安全技术要求》标准的修订遵循以下原则：

(1) 先进性：标准反映当今路由器安全的先进技术水平；

(2) 开放性：标准的修订、评审与使用具有开放性；

(3) 适应性：标准结合我国国情；

(4) 简明性：标准易于理解、实现和应用；

(5) 中立性：公正、中立，不与任何利益攸关方发生关联；

(6) 一致性：术语与国内外标准所用术语最大程度保持一致。

2.2 主要修订内容

本标准与GB/T 18018－2007的主要差异如下：

——“2 规范性引用文件”进行了更新；

——“3.2 缩略语”中补充了内容；

——“4 第一级安全要求”中修改了“4.1.2.1 管理员鉴别”；

——“4 第一级安全要求”中增加了“4.1.3.2 管理协议设置”、“4.1.4 设备安全防护”和“4.1.5 安全功能保护”；

——“5 第二级安全要求”中修改了“5.1.2.1 管理员鉴别”和“5.1.3.1 权限管理”；

——“5 第二级安全要求”中增加了“5.1.3.2 管理协议设置”、“5.1.4 设备安全防护”、“5.1.5 网络安全防护” 和“5.1.6 安全功能保护”；

——“5.1.8 路由认证”调整为本标准中的“5.1.5.2 路由协议认证”；

——“6 第三级安全要求”中修改了“6.1.2.1 管理员鉴别”和“6.1.4.1 权限管理”；

——“6 第三级安全要求”中增加了“6.1.2.2 设备登录口令管理”、“6.1.2.3 证书验证”、“6.1.3.2 数据存储”、“6.1.3.3 数据传输”、“6.1.3.4 敏感数据”、“6.1.4.2 管理协议设置”、“6.1.5　设备安全防护”、“6.1.6 网络安全防护”和“6.1.7　安全功能保护”；

—— 删除了GB/T 18018—2007的“5.1.8 路由认证”和“6.1.10 路由认证”；分别调整到本标准的相应章节之中。

——“附录A”的“A.1 安全功能要求对照表”中增加“设备安全防护”行及相应的3个子行；

——“附录A”的“A.1 安全功能要求对照表”中增加“网络安全防护”行及相应的3个子行；

——“附录A”的“A.1 安全功能要求对照表”中的“身份鉴别”行中增加2个子行；

——“附录A”的“A.1 安全功能要求对照表”中的“数据保护”行中增加3个子行；

——“附录A”的“A.1 安全功能要求对照表”中的“安全管理”行中增加2个子行；

1. 主要试验（或验证）的分析、综述报告、技术经济论证、预期的经济效果

修订组中的企业，包括华为技术有限公司、新华三技术有限公司和迈普通信技术股份有限公司具有长期研制路由器的经验。他们对修订后的标准进行试用与验证，取得初步成果，目前进展良好。反馈的建议对标准的修订奠定了良好基础。

1. 采用国际标准和国外先进标准的程度、以及与国际、国外同类标准水平的对比情况、或与测试的国外样品、样机的有关数据对比情况

路由器是网络通信中广泛应用的骨干设备，其安全性和安全应用具有重要意义。我们在前一个版本的基础上，广泛参考了国内外的相关标准和规范，结合目前的技术发展、我国的应用实践进行修改、补充与完善。提出与国际标准接轨、适合我国国情的“路由器安全技术要求”标准。

1. 与有关的现行法律、法规和强制性国家标准的关系

本标准符合现有法律法规的要求。

1. 重大分歧意见的处理经过和依据

本标准在修订过程中未出现重大分歧，其他详见意见汇总处理表。

1. 国家标准作为强制性国家标准或推荐性国家标准的建议

建议本标准作为推荐性国家标准发布实施。

1. 贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）

本标准作为路由器安全标准体系的一部分，配合实施。

1. 其他事项说明

本标准不涉及专利。

标准修订组 2017年8月