ICS 35.040
CCS L 80

中华人民共和国国家标准

GB/T 41268—2022

网络关键设备安全检测方法
路由器设备

Security testing methods for critical network devices—Router

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

GB 40050—2021《网络关键设备安全通用要求》与GB/T 41269—2022《网络关键设备安全技术要求　路由器设备》、GB/T 41268—2022《网络关键设备安全检测方法　路由器设备》共同构成支撑网络关键设备的路由器设备安全标准体系。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、启明星辰信息技术集团股份有限公司、上海诺基亚贝尔股份有限公司、北京奇虎科技有限公司、中国联合网络通信集团有限公司、中兴通讯股份有限公司、北京通和实益电信科学技术研究所有限公司、新华三技术有限公司、烽火通信科技股份有限公司、中国通信标准化协会。

本文件主要起草人：张治兵、周开波、王卫东、程小平、周继华、万晓兰、邱林海、张屹、郭新海、吴荣春、叶郁柏、孙薇、李海英、姚一楠、张亚薇、柳扬、马铮、吴萍、袁玉东、陆强、薄菁、刘欣东、邓科、苏燕谨。

网络关键设备安全检测方法
路由器设备

1 范围

本文件给出了列入网络关键设备的路由器设备在标识安全、冗余、备份恢复与异常检测、漏洞与缺陷管理、预装软件启动及更新安全、默认状态安全、抵御常见攻击能力、用户身份标识与鉴别安全、访问控制安全、日志审计安全、通信安全、数据安全等方面的安全功能要求的检测方法，以及上述设备在设计和开发、生产和交付、运行和维护三个阶段的安全保障要求的评估方法。

本文件适用于列入网络关键设备目录的路由器设备，也可为网络运营者采购路由器设备时提供依据，还适用于指导路由器设备的研发、测试等工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069 信息安全技术 术语

GB 40050—2021 网络关键设备安全通用要求

3GPP TS 33.117 通用安全保障要求(Catalogue of general security assurance requirements)

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

路由器 router

用来建立和控制不同网络间数据流的网络设备。

注：路由器基于路由协议机制和算法来选择路径或路由以实现建立和控制网络间的数据流，网络自身可以基于不同的网络协议。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表(Access Control List)

ARP：地址解析协议(Address Resolution Protocol)

BGP：边界网关协议(Border Gateway Protocol)

DHCP：动态主机配置协议(Dynamic Host Configuration Protocol)

FTP：文件传输协议(File Transfer Protocol)

HTTP：超文本传输协议(Hyper Text Transfer Protocol)