ICS 35.040
CCS L 80

中华人民共和国国家标准

GB 42250—2022

信息安全技术
网络安全专用产品安全技术要求

Information security technology—
Security technical requirements of specialized cybersecurity products

2022-12-29 发布　　2023-07-01 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 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　安全功能要求 …… 2
4.1　访问控制 …… 2
4.2　入侵防范 …… 2
4.3　安全审计 …… 2
4.4　恶意程序防范 …… 2
5　自身安全要求 …… 3
5.1　标识和鉴别 …… 3
5.2　自身访问控制 …… 3
5.3　自身安全审计 …… 3
5.4　通信安全 …… 3
5.5　支撑系统安全 …… 3
5.6　产品升级 …… 3
5.7　用户信息安全 …… 3
5.8　密码要求 …… 4
6　安全保障要求 …… 4
6.1　供应链安全 …… 4
6.2　设计与开发 …… 4
6.3　生产和交付 …… 4
6.4　运维服务保障 …… 4
6.5　用户信息保护 …… 5
参考文献 …… 6

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。

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公安部提出并归口。

引　言

为落实《中华人民共和国网络安全法》的第二十三条而制定本文件。网络安全专用产品按照本文件的安全技术要求和国家相关主管部门规定的其他技术规范进行研发、生产、服务和检测工作。

本文件是所有网络安全专用产品和其提供者均需满足的基线要求。

信息安全技术
网络安全专用产品安全技术要求

1 范围

本文件规定了网络安全专用产品的安全功能要求、自身安全要求与安全保障要求。

本文件适用于销售或提供的网络安全专用产品的研发、生产、服务、检测。

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标准；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

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

网络安全专用产品 specialized cybersecurity products

用于保护网络安全的专用硬件和软件产品。

注：包括以服务形式提供安全防护能力的产品。

3.2

网络安全专用产品提供者 specialized cybersecurity products provider

网络安全专用产品的研发者、生产者或维护服务提供者。

3.3

安全域 security domain

遵从共同安全策略的资产和资源的集合。

[来源：GB/T 25069—2022，3.36]

3.4

个人信息 personal information

以电子方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.5

用户信息 user information

个人、法人或其他组织在安装、使用网络安全专用产品过程中产生、收集、存储、传输、处理的电子方式记录的信息。

注：用户信息包括网络流量信息、安全状态信息、安全配置数据、运行过程日志等信息，也包括个人信息。

3.6

恶意程序　malicious program

具有破坏网络和信息系统、干扰网络和信息系统正常使用、窃取或恶意加密网络和系统数据等网络攻击功能的程序。

注：恶意程序主要包括病毒、蠕虫、木马，以及其他影响主机、网络或系统安全、稳定运行的程序。

3.7

安全缺陷　security flaw

由设计、开发、配置、生产、运维等阶段中的错误引入，可能影响网络安全专用产品安全的弱点。

3.8

漏洞　vulnerability

网络安全专用产品中能够被威胁利用的弱点。

4　安全功能要求

4.1　访问控制

具有访问控制功能的网络安全专用产品，应具备下述功能：

a）　支持配置访问控制策略；

注：不同类型网络安全专用产品的访问控制策略不同。如：网络型防火墙基于源地址、目的地址、源端口、目的端口和网络通信协议等设置访问控制策略；虚拟专用网类产品基于用户安全属性等设置访问控制策略；安全隔离与信息交换类产品基于应用层协议等设置访问控制策略。

b）　支持根据访问控制策略控制对安全域的访问。

4.2　入侵防范

具有入侵防范功能的网络安全专用产品，应具备下述功能：

a）　支持对收集的信息进行分析，发现入侵事件；

b）　在检测到入侵事件时，支持采取记录事件、安全警告或阻断等安全措施。

4.3　安全审计

具有安全审计功能的网络安全专用产品，应具备下述功能：

a）　支持监测、记录审计目标的网络运行状态、网络安全事件；

注：不同类型网络安全专用产品的安全审计目标不同，审计目标通常包括主机、网络、数据库、应用等。

b）　支持对事件进行比较分析以发现违规、异常等行为；

c）　将网络运行状态日志和网络安全事件日志存储于非易失性存储介质中，日志保存时间不少于六个月。

4.4　恶意程序防范

具有恶意程序防范功能的网络安全专用产品，应具备下述功能：

a）　支持对存储信息或传输信息进行恶意程序检测；

注：存储信息包括但不限于存储于主机磁盘、主机内存、主机引导区、移动存储介质中的信息；传输信息包括但不限于通过通信协议传输信道传输的文件数据或程序代码。

b）　支持针对一种或多种恶意程序家族类型进行检测；

c）　支持对检测到的恶意程序进行阻止、删除、修复或隔离等一种或多种形式的处理。

5 自身安全要求

5.1 标识和鉴别

网络安全专用产品应具备下述功能：

a) 对用户身份进行标识和鉴别，身份标识具有唯一性；

b) 保障身份鉴别信息在传输和存储过程中的保密性和完整性；

c) 使用口令鉴别方式时，提供身份鉴别信息复杂度验证功能和定期更换设置功能，并支持首次管理产品时强制修改默认口令或设置口令。

5.2 自身访问控制

网络安全专用产品应具备下述功能：

a) 对用户分配账户和权限，区分管理员角色，实现管理权限相互制约；

b) 由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

5.3 自身安全审计

网络安全专用产品应具备下述功能：

a) 监测、记录产品自身运行状态和重要操作；

b) 对审计日志进行保护，防止受到未预期的删除、修改、覆盖或丢失；

c) 将审计日志存储于非易失性存储介质中，日志保存时间不少于六个月。

5.4 通信安全

网络安全专用产品应提供安全措施保障产品远程管理网络通信数据的保密性和完整性。

5.5 支撑系统安全

网络安全专用产品不应包含已公开的中、高风险漏洞。

注：漏洞风险等级参照国家网络安全漏洞分类分级指南(如 GB/T 30279 等标准)等国家有关规定。

5.6 产品升级

网络安全专用产品应具备下述功能：

a) 提供升级产品组件的功能，包括但不限于主程序、特征库、策略库；

b) 保障升级安全，避免得到错误的、伪造的升级包和补丁程序。

5.7 用户信息安全

网络安全专用产品应具备下述功能：

a) 仅收集实现产品功能所必需的用户信息；

b) 在涉及个人信息处理时提供相关授权功能，在获得授权后方能处理个人信息；

注 1：个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。授权功能包括但不限于个人信息收集前的授权同意、个人信息收集的授权撤回等。

c) 在未获得或撤回个人信息收集授权的情况下提供与个人信息无关的安全功能；

d) 在涉及个人信息传输和存储的过程中保障个人信息的保密性和完整性；

e) 在涉及个人信息存储时提供对超出保存期限个人信息的处理功能。

注 2：对超出保存期限个人信息的处理方式应与用户授权的处理方式一致，如采取删除或匿名化处理措施。

5.8 密码要求

本文件凡涉及密码使用和管理的相关内容，按有关标准的规定。

6 安全保障要求

6.1 供应链安全

网络安全专用产品提供者应满足以下安全保障要求：

a） 制定供应商选择、评定和日常管理的程序，对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出管理要求，以确保其提供的关键部件满足安全要求，并保存对供应商选择、评价和日常管理的记录；

b） 建立供应链各环节核心要素的追溯能力，保障核心要素供应稳定；

注：核心要素包括核心技术知识产权、工具及部件等。核心技术知识产权如源代码、软硬件设计图等；工具如开发软件、编译软件、测试软件、测试仪表、管理软件、拷机软件等；部件如硬件机箱、操作系统等。

c） 持续开展安全意识和技能培训。

6.2 设计与开发

网络安全专用产品提供者应满足以下安全保障要求：

a） 识别网络安全专用产品设计和开发环节的安全风险，进行威胁建模，制定安全策略，保障开发环境安全，制定安全开发制度和流程；

注 1：安全开发制度和流程包括但不限于代码编写规范、研发环境安全管理制度、研发人员安全管理制度、研发交付制度等。

b） 制定网络安全专用产品安全功能和自身安全功能的设计文档，该文档描述与安全功能和自身安全功能一致；

c） 为网络安全专用产品确定唯一的版本号，为配置项确定唯一标识，建立并维护配置项列表；

注 2：配置项包括但不限于源代码、工具、文档、组件、配置信息等。

d） 不在产品中设置恶意程序、隐蔽接口或未明示功能模块等，并通过用户协议、产品说明书等途径将所有功能模块、接口等告知用户；

e） 对网络安全专用产品进行安全性测试。

注 3：安全性测试包括但不限于漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证等。

6.3 生产和交付

网络安全专用产品提供者应满足以下安全保障要求：

a） 建立和执行规范的产品完整性检测流程，采取措施防范自制或采购的组件被篡改、伪造等风险；

b） 建立内部交付和外部交付的控制程序，确保网络安全专用产品在交付过程中不被破坏或篡改；

c） 向用户明示包含在产品中的所有功能模块、外部接口和私有协议，告知用户产品中预置的所有账户和默认口令。

6.4 运维服务保障

网络安全专用产品提供者应满足以下安全保障要求：

a) 在法律法规规定或与用户约定的期限内，为产品提供持续的安全维护，不单方面中断或终止安全维护；
b) 保护用户对软件（包含固件）安装和升级等的知情权和选择权，安装和升级软件时明示用户并获得用户同意；
c) 建立和执行针对产品安全缺陷、漏洞的应急响应机制和流程，对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施，及时告知用户安全风险和可用的补救措施，并向有关主管部门报告。

6.5 用户信息保护

网络安全专用产品提供者应满足以下安全保障要求：

a) 明示收集用户信息的目的、方式、范围、种类、存储位置和处理方式；
b) 建立和执行用户信息管理制度和流程，在产品设计、生产、升级等各阶段保障用户信息的安全，不超范围使用用户信息。

参 考 文 献

[1] GB 17859—1999 计算机信息系统 安全保护等级划分准则
[2] GB/T 30279 信息安全技术 网络安全漏洞分类分级指南
[3] 中华人民共和国网络安全法
[4] 中华人民共和国密码法
[5] 中华人民共和国数据安全法
[6] 中华人民共和国产品质量法
[7] 中华人民共和国消费者权益保护法
[8] 中华人民共和国个人信息保护法
[9] 中华人民共和国计算机信息系统安全保护条例
[10] 关键信息基础设施安全保护条例
[11] 国务院关于印发新时期促进集成电路产业和软件产业高质量发展若干政策的通知(国发〔2020〕8号)