ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39276—2020

信息安全技术
网络产品和服务安全通用要求

Information security technology—
General security requirements of network products and services

2020-11-19 发布　　2021-06-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、北京赛西科技发展有限责任公司、公安部第三研究所、中国信息安全测评中心、中国网络安全审查技术与认证中心、国家信息技术安全研究中心、中国电子信息产业发展研究院、中国科学院信息工程研究所、中国信息通信研究院、国家信息中心、国家计算机网络与信息安全管理中心、中电数据服务有限公司、中国软件评测中心、工业和信息化部电子第五研究所、中国电子科技集团公司第十五研究所、中国科学院软件研究所、公安部第一研究所、阿里巴巴(北京)软件服务有限公司、联想(北京)有限公司、阿里云计算有限公司、浪潮电子信息产业股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司、启明星辰信息技术集团股份有限公司、中国电力科学研究院有限公司、北京神州绿盟科技有限公司、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京威努特技术有限公司、山谷网安科技股份有限公司、国家应用软件产品质量监督检验中心、新华三技术有限公司、浙江蚂蚁小微金融服务集团股份有限公司、深信服科技股份有限公司、西门子(中国)有限公司、奇安信科技集团股份有限公司。

本标准主要起草人:刘贤刚、李京春、顾健、李斌、李嵩、叶润国、孙彦、谢安明、胡影、王闯、许东阳、高金萍、宋好好、周开波、舒敏、吴迪、刘蓓、何延哲、方进社、崔宁宁、周亚超、张宝峰、布宁、任泽君、申永波、李汝鑫、樊洞阳、雷晓锋、鲍旭华、程广明、郭永振、白晓媛、赵江、杜晓黎、史岗、韩煜、董晶晶、刘玉岭、李凌、李娜、严妍、徐雨晴、张屹、焦玉峰、代威、石凌志、钟建伟、姚金龙、宋铮、闫韬、郭旭、王晖。

信息安全技术
网络产品和服务安全通用要求

1 范围

本标准规定了网络产品和服务应满足的安全通用要求，包括安全功能要求和安全保障要求。

本标准适用于网络产品和服务提供者进行网络产品和服务的安全设计、安全实现和安全运行，也可用于指导第三方测评机构对网络产品和服务进行安全测评。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 network

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.2

网络产品 network product

作为网络组成部分以及实现网络功能的硬件、软件或系统，按照一定的规则和程序实现信息的收集、存储、传输、交换和处理。

注：网络产品包括计算机、通信设备、信息终端、工控网络设备、系统软件和应用软件等。

3.3

用户信息 user information

与个人、法人或其他组织有关的信息，以及定义和描述此类信息的数据。

注：用户信息包括个人信息，用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生的日志等。

3.4

恶意程序 malware

用于实施网络攻击、干扰网络和信息系统正常使用、破坏网络和信息系统、窃取网络和系统数据等行为的程序。

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。

3.5

安全缺陷 security flaw

由设计、开发、配置、生产、运维等阶段中的问题引入，可能影响网络产品和服务安全的弱点。

3.6

漏洞　vulnerability

网络产品和服务中能够被威胁利用的弱点。

注：改写 GB/T 25069—2010，定义 2.3.30。

4　概述

网络产品和服务的安全直接影响到其支撑的网络的安全。网络产品和服务在研发、生产、交付、服务提供或运维过程中可能引入安全隐患，导致信息泄露、数据篡改、服务中断、不当控制等安全风险。为了减少网络产品和服务中的常见安全风险，提升用户对网络产品和服务在安全性方面的信心，网络产品和服务提供者应采取相应安全措施，实现以下安全目标：

a）防范信息泄露风险：保障网络产品和服务中用户信息不被泄露，降低用户信息泄露的安全风险；

b）防范数据篡改风险：保障网络产品和服务中用户信息不被非授权更改或伪造，降低数据被篡改的安全风险；

c）防范服务中断风险：保障网络产品和服务的持续运行和供应，降低网络产品和服务供应中断的安全风险；

d）防范不当控制风险：保障网络产品和服务运行过程中的风险可控，降低网络产品和服务提供者恶意控制用户的网络产品和服务、非授权获取用户信息，以及利用用户对网络产品和服务的依赖实施不正当竞争或损害用户利益的风险。

本标准从安全功能和安全保障两个方面规范网络产品和服务的安全通用要求。安全功能和安全保障均包含基本级和增强级安全要求，其中增强级安全要求用**宋体粗体字**进行标识。

5　安全通用要求

5.1　基本级安全通用要求

5.1.1　安全功能要求

5.1.1.1　身份标识和鉴别

具有用户身份标识和鉴别功能的网络产品和服务应：

a）对用户身份进行标识和鉴别，身份标识具有唯一性；

b）对用户身份鉴别凭证进行安全保护，防止鉴别凭证的泄露、篡改；

c）告知用户网络产品和服务中与用户相关的所有预置的账户和默认口令，允许用户更改默认口令；

d）在存在默认口令时，提示用户对默认口令进行修改。

5.1.1.2　授权与访问控制

具有授权与访问控制功能的网络产品和服务应：

a）按照最小授权原则，在出厂时预置访问控制策略，需要配置安全策略时，允许用户更改访问控制策略；

b）在用户访问受控资源或功能时，依据设置的访问控制策略进行访问控制，保障访问和操作的安全；

c）不存在加载或运行后会禁用或绕过访问控制机制的组件。

5.1.1.3 日志记录与审计

具有日志记录与审计功能的网络产品和服务应：

a) 对用户账户的登录、注销、系统开关机和核心配置变更等操作进行日志记录；
b) 在日志记录中包括事件发生的日期和时间、事件的类型、主体身份、事件操作结果等；
c) 对日志记录进行安全保护，防止日志记录的损毁或未授权的追加、访问、修改、删除等。

5.1.1.4 用户信息安全保护

具有用户信息收集、处理等功能的网络产品和服务应：

a) 除法律法规另有规定外，明确告知收集用户信息的目的、用途、范围和类型，在获得用户同意后，方可收集用户信息；
b) 将收集的用户信息仅用于用户同意的目的和用途；
c) 在收集实现网络产品和服务功能所需的用户信息时遵循最小化原则；
d) 采取安全措施保护个人信息等重要用户信息的安全，防止泄露、篡改、损毁、丢失；
e) 未经用户同意，不得向他人提供可精确定位到特定个人的信息；
f) 在符合法律法规且技术可行条件下，向用户提供查询、更正个人信息的功能；
g) 在报废或终止后，按法律法规、用户要求对用户信息进行处理，或删除用户信息。

5.1.1.5 密码使用与管理

采用了密码技术的网络产品和服务应符合国家密码管理相关规定。

5.1.2 安全保障要求

5.1.2.1 设计和开发

网络产品和服务的提供者应：

a) 制定和实施网络产品和服务安全开发流程，减少设计、开发等过程中恶意程序植入、漏洞引入的风险；
b) 对设计文档、开发文档等进行配置管理，建立配置管理清单或相应程序，对配置项的变更进行授权和控制；
c) 识别网络产品和服务在设计、开发环节的安全风险，制定安全策略，采取安全措施保障关键组件的设计和开发安全；
d) 自行、联合或委托第三方对网络产品和服务（包括网络产品和服务中使用的第三方软硬件模块）进行安全测试；
e) 在开发阶段对已发现的安全缺陷、漏洞进行修复，对于不能在开发阶段及时修复的安全缺陷、漏洞，制定并实施在用户侧进行紧急修复的安全管理流程。

5.1.2.2 生产和交付

网络产品和服务提供者应：

a) 采取完整性保护措施降低网络产品和服务中关键组件、过程和数据被篡改、伪造的风险，包括但不限于对使用的第三方软硬件模块进行安全性检测等；
b) 向用户说明包含在网络产品和服务中的所有与用户相关的功能模块和访问接口，包括但不限于人机接口、调试接口等；
c) 通过用户协议、产品使用说明书或网站通报等途径，声明所提供的网络产品和服务中没有故意

留有或者设置漏洞、后门、木马等程序和功能。

5.1.2.3 运行和维护

网络产品和服务提供者应：

a) 建立和执行针对网络产品和服务安全缺陷、漏洞的应急响应机制和流程，对网络产品和服务在运行和维护阶段暴露的安全缺陷、漏洞进行响应；

b) 发现网络产品和服务存在安全缺陷、漏洞时，立即采取修复或替代方案等补救措施，按照国家网络安全监测预警和信息通报制度等相关规定，及时告知用户安全风险，并向有关主管部门报告；

c) 在法律法规规定或与用户约定的期限内，为网络产品和服务提供持续的安全维护，不因业务变更、产权变更等原因单方面中断或终止安全维护；

d) 建立和实施规范的用户信息保护制度，当存在违反法律法规规定或者双方约定收集、使用用户个人信息的情形时，应主动或在用户要求下删除个人信息；

e) 保护用户对软件安装、使用、升级、卸载的知情权和选择权，安装和升级软件时应明示告知用户并获得用户同意，允许用户卸载或禁用完成业务目标所必备产品核心功能之外的软件，不得强制或诱导用户安装或升级用户不知情的软件。

5.2 增强级安全通用要求

5.2.1 安全功能要求

5.2.1.1 身份标识和鉴别

具有用户身份标识和鉴别功能的网络产品和服务应：

a) 对用户身份进行标识和鉴别，身份标识具有唯一性；

b) 对用户身份鉴别凭证进行安全保护，防止鉴别凭证的泄露、篡改；

c) 告知用户网络产品和服务中与用户相关的所有预置的账户和默认口令，允许用户更改默认口令；

d) 在未修改默认口令时，限制核心功能的使用，并提示用户修改口令；

e) 在采用基于口令的身份鉴别机制时，对用户设置的口令进行复杂度检查；

f) 具有登录失败和超时安全处理等机制，包括但不限于连续登录失败后锁定用户账户，当发生用户会话连接超时自动退出用户会话等。

5.2.1.2 授权与访问控制

具有授权与访问控制功能的网络产品和服务应：

a) 按照最小授权原则，在出厂时预置访问控制策略，需要配置安全策略时，允许用户更改访问控制策略；

b) 在用户访问受控资源或功能时，依据设置的访问控制策略进行访问控制，保障访问和操作的安全；

c) 不存在加载或运行后会禁用或绕过访问控制机制的组件；

d) 支持对不同用户账号或应用软件授予完成各自承担任务所需的最小访问权限。

5.2.1.3 日志记录与审计

具有日志记录与审计功能的网络产品和服务应：

a) 对用户账户的登录、注销、系统开关机和核心配置变更等操作进行日志记录；

b) 在日志记录中包括事件发生的日期和时间、事件的类型、主体身份、事件操作结果等；
c) 对日志记录进行安全保护，防止日志记录的损毁或未授权的追加、访问、修改、删除等；
d) 提供设置日志记录存储容量、保存时间的功能，日志保存时间应满足国家有关规定。

5.2.1.4 信息通信安全保护

具有信息通信安全保护功能的网络产品和服务应：
a) 在通信双方建立网络连接时，验证通信端身份真实性；
b) 提供安全措施保障通信数据的保密性、完整性、可用性；
c) 保障通信协议的安全性，可抵御常见的重放攻击、中间人攻击等安全威胁。

5.2.1.5 用户信息安全保护

具有用户信息收集、处理等功能的网络产品和服务应：
a) 除法律法规另有规定外，明确告知收集用户信息的目的、用途、范围和类型，在获得用户同意后，方可收集用户信息；
b) 将收集的用户信息仅用于用户同意的目的和用途；
c) 在收集实现网络产品和服务功能所需的用户信息时遵循最小化原则；
d) 采取安全措施保护个人信息等重要用户信息的安全，防止泄露、篡改、损毁、丢失；
e) 未经用户同意，不得向他人提供可精确定位到特定个人的信息；
f) 在符合法律法规且技术可行条件下，向用户提供查询、更正个人信息的功能；
g) 在报废或终止后，按法律法规、用户要求对用户信息进行处理，或删除用户信息；
h) 在传输和存储个人敏感信息时，采取加密等安全措施。

5.2.1.6 密码使用与管理

采用了密码技术的网络产品和服务应符合国家密码管理相关规定。

5.2.2 安全保障要求

5.2.2.1 设计和开发

网络产品和服务的提供者应：
a) 制定和实施网络产品和服务安全开发流程，减少设计、开发等过程中恶意程序植入、漏洞引入的风险；
b) 对设计文档、开发文档等进行配置管理，建立配置管理清单或相应程序，对配置项的变更进行授权和控制；
c) 识别网络产品和服务在设计、开发环节的安全风险，制定安全策略，采取安全措施保障关键组件的设计和开发安全；
d) 自行、联合或委托第三方对网络产品和服务（包括网络产品和服务中使用的第三方软硬件模块）进行安全测试；
e) 在开发阶段对已发现的安全缺陷、漏洞进行修复，对于不能在开发阶段及时修复的安全缺陷、漏洞，制定并实施在用户侧进行紧急修复的安全管理流程；
f) 提供设计与实现之间的对应关系，并证明其一致性。

5.2.2.2 生产和交付

网络产品和服务提供者应：

a) 采取完整性保护措施降低网络产品和服务中关键组件、过程和数据被篡改、伪造的风险，包括但不限于对使用的第三方软硬件模块进行安全性检测等；
b) 向用户说明包含在网络产品和服务中的所有与用户相关的功能模块和访问接口，包括但不限于人机接口、调试接口等；
c) 通过用户协议、产品使用说明书或网站通报等途径，声明所提供的网络产品和服务中没有故意留有或者设置漏洞、后门、木马等程序和功能；
d) 建立和实施规范的产品生产和服务交付流程，在关键环节实施安全检查和验证，减少产品生产和服务交付过程中的安全风险；
e) 为用户提供验证所交付产品完整性必需的安全措施，减少产品交付过程中的篡改风险；
f) 为用户提供操作指南等指导性文档，明确产品典型部署环境应满足的安全要求，描述产品使用过程中涉及的各用户角色和安全责任，给出风险提示和应急响应措施。

5.2.2.3 运行和维护

网络产品和服务提供者应：

a) 建立和执行针对网络产品和服务安全缺陷、漏洞的应急响应机制和流程，对网络产品和服务在运行和维护阶段暴露的安全缺陷、漏洞进行响应。
b) 发现网络产品和服务存在安全缺陷、漏洞时，立即采取修复或替代方案等补救措施，按照国家网络安全监测预警和信息通报制度等相关规定，及时告知用户安全风险，并向有关主管部门报告。
c) 在法律法规规定或与用户约定的期限内，为网络产品和服务提供持续的安全维护，不因业务变更、产权变更等原因单方面中断或终止安全维护。
d) 建立和实施规范的用户信息保护制度，当存在违反法律法规规定或者双方约定收集、使用用户个人信息的情形时，应主动或在用户要求下删除个人信息。
e) 保护用户对软件安装、使用、升级、卸载的知情权和选择权，安装和升级软件时应明示告知用户并获得用户同意，允许用户卸载或禁用完成业务目标所必备产品核心功能之外的软件，不得强制或诱导用户安装或升级用户不知情的软件。
f) 在对产品和服务的安全缺陷、漏洞进行修复时，提前告知用户将采取的处置操作和可能产生的影响。
g) 为用户信息在不同网络产品和服务间迁移提供必要的技术支持，允许用户导出或备份用户信息。
h) 在远程维护网络产品前，明确告知用户远程维护的目的和范围，并获得用户授权同意。为用户提供中止网络产品远程维护的方式。远程维护中止或结束时，远程维护权限自动撤销。
i) 在远程维护网络产品时，在用户侧显示提示信息，记录远程维护的所有操作，生成审计日志供用户查阅。
j) 在升级网络产品和服务前告知用户升级的内容，包括变更情况、相关安全风险、风险应对措施等，获得用户授权同意后方可实施升级，允许用户选择不接受升级。
k) 在用户需要时，为用户提供支持网络产品和服务升级包的完整性、来源真实性等安全校验的方法或工具。
l) 保护网络产品和服务在运行维护过程中的用户信息，防止用户信息泄露、篡改、损毁、丢失。
m) 在跨境传输个人信息和重要数据时，符合国家数据出境管理有关规定。

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件

[3] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

[4] GB/T 28827.1—2012 信息技术服务 运行维护 第1部分:通用要求

[5] GB/T 28827.2—2012 信息技术服务 运行维护 第2部分:交付规范

[6] GB/T 28827.3—2012 信息技术服务 运行维护 第3部分:应急响应规范

[7] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则

[8] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[9] GB/T 35273—2020 信息安全技术 个人信息安全规范