ICS 33.050
CCS M 30

团　体　标　准

T/TAF 249—2024

网络产品操作系统内核安全技术要求

Security technical requirements for operating system kernel of network products

2024-09-02 发布　　2024-09-02 实施

电信终端产业协会　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　操作系统内核概述 2
6　安全功能分级 2
7　安全技术要求 2
7.1　完整性保护要求 2
7.2　隔离要求 3
7.3　访问控制要求 3
7.4　存储安全要求 4
7.5　通信安全要求 5
7.6　密码安全要求 5
7.7　自保护要求 6
7.8　日志审计要求 6
附录 A（规范性）　安全等级划分 8
附录 B（资料性）　安全风险分析 10
B.1　安全资产 10
B.2　安全风险 10
参考文献 11

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、锐捷网络股份有限公司、武汉网锐检测科技有限公司、浪潮电子信息产业股份有限公司、联想（北京）有限公司、博鼎实华（北京）技术有限公司。

本文件主要起草人：刘欣东、路晔绵、吴荣春、刘哲、马宇航、李革飞、周继华、杨小锦、李伟滨、赵新星、龚志红、陈玺、刘波、许鑫、刘俊、刘刚、刘向东。

网络产品操作系统内核安全技术要求

1 范围

本文件规定了针对网络产品操作系统内核的安全技术要求，主要包括完整性保护要求、隔离要求、访问控制要求、存储安全要求、通信安全要求、密码安全要求、自保护要求、日志审计要求等。

本文件适用于网络产品操作系统内核的研发、测试、评估与认证。

本文件中的网络产品适用范围包括提供网络功能的操作系统、软件、具有操作系统功能或特征的硬件（如网络设备、计算设备等），也适用于信息终端产品。

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 25069-2022 信息安全技术 术语

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

操作系统内核 operating system kernel

操作系统中负责系统进程、内存、设备驱动、文件和网络系统等核心功能的计算机程序。

[来源：GB/T 36630.3-2018，3.2]

3.2

内核服务 kernel service

操作系统内核通过系统调用方式向应用程序提供的功能，可以包括内存分配、进程调度、设备驱动、文件系统访问等。

3.3

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。

[来源：GB/T 39276-2020，3.2]

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

ASLR：地址空间布局随机化（Address Space Layout Randomization）

DFI：动态流检测（Dynamic Flow Inspection）

5 操作系统内核概述

操作系统内核是网络产品操作系统/软件部分的核心，是基于硬件的第一层软件扩充，提供操作系统的最基本的功能，是操作系统工作的基础。

操作系统内核是软硬件系统的中枢，负责管理系统的硬件和软件资源，包括系统的进程、内存、设备驱动程序、文件和网络系统，其决定着系统的性能和稳定性。

6 安全功能分级

网络产品操作系统内核安全风险分析可见附录B。

可根据应对的安全风险将网络产品操作系统内核安全技术要求分为三个等级，不同级别的安全功能如下：

——一级安全要求（基本级）：应能够防护少量未授权的用户对操作系统内核发起恶意攻击所造成的关键资源损害，能够对用户态与内核态内存和资源隔离，能够提供基础级的访问控制，能够存储记录安全事件以供审计和分析功能；

——二级安全要求（增强级）：应能够防护一定数量未授权的用户对操作系统内核发起恶意攻击所造成的关键资源损害，能够提供操作系统内核完整性保护机制，能够提供细颗粒度和强制访问控制功能，能够提供用户态进程的特殊安全和密码功能，能够对入侵检测事件进行监控和收集以供分析；

——三级安全要求（卓越级）：应能够防护大量未授权的用户对操作系统内核发起恶意攻击所造成的关键资源损害，能够从多个层面限制攻击者的访问能力，能够提供虚拟化和容器隔离功能，具备内核服务隔离机制，具备采取一定手段限制攻击者利用漏洞的能力。

各等级对应的条款见附录A。

7 安全技术要求

7.1 完整性保护要求

7.1.1 架构支持

网络产品操作系统内核架构应支持对用户态服务进程、内核扩展模块的完整性度量。

7.1.2 启动时完整性保护

网络产品操作系统内核应支持以下启动时完整性保护机制：

a) 应支持在加载预置可执行文件时进行完整性检验；

b) 应支持在加载动态扩展的可执行文件时进行完整性校验，例如升级包完整性检验。

7.1.3 运行时完整性保护

网络产品操作系统内核应支持以下运行时完整性保护机制：

a） 应支持只读文件完整性保护机制，在用户态进程读取只读文件时，操作系统内核应支持对读取内容进行完整性校验，确保读取的内容未被篡改；
b） 应支持全盘文件系统完整性保护机制，确保读取内容的完整性；
c） 应支持代码段完整性保护机制，对可执行文件代码段在其生命周期内进行完整性保护，保护其不被篡改；
d） 应支持数据流完整性保护，如支持DFI防护能力；
e） 应支持前向控制流完整性保护，限制程序运行中的控制流转移，使其始终处于原有的控制流图所限定的范围内；
f） 应支持后向控制流完整性保护，保护返回指令的控制流转移的完整性，使其始终处于原有的控制流图所限定的范围内。

7.1.4 完整性度量值存储

网络产品操作系统内核应支持完整性度量基准值的可信存储，防止其被篡改。

7.2 隔离要求

7.2.1 用户态与内核态隔离

网络产品操作系统内核应支持用户态与内核态内存空间和资源隔离。

7.2.2 用户态隔离支持

网络产品操作系统内核应提供用户态不同进程之间内存空间和资源的隔离机制。

7.2.3 虚拟化隔离

网络产品操作系统内核支持虚拟化时，应保证不同虚拟机间内存空间和资源的隔离。

7.2.4 容器隔离

网络产品操作系统内核提供容器技术时，应保证容器中业务的内存空间与容器外隔离。

7.2.5 用户隔离

网络产品操作系统内核应实现不同用户的资源隔离。

7.2.6 内核服务隔离

网络产品操作系统内核应支持以下内核服务隔离机制：
a） 应支持内核服务之间内存空间和资源隔离；
b） 应保证服务出现故障重启时，不影响其他服务的正常运行；
c） 应限制攻击对内核服务的影响，如：驱动地址空间隔离、页表隔离等。

7.3 访问控制要求

7.3.1 自主访问控制

网络产品操作系统内核应提供如下自主访问控制机制：
a） 客体的拥有者对其拥有的全部客体应有权修改其访问权限；
b） 客体的拥有者应能对其拥有的客体设置其他同组用户的访问控制属性，访问控制属性包含但不限于读、写、执行等；

c） 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性包含但不限于读、写、执行等；
d） 主体对客体的访问应遵循该客体的自主访问控制权限属性；
e） 客体的拥有者应能对其拥有的客体设置单个用户或组的访问控制属性，访问控制属性包括但不限于读、写、执行等；
f） 客体的拥有者应能将访问控制客体的颗粒度控制在文件和目录；
g） 创建客体时，该客体应具有该主体设置的自主访问控制权限属性的默认值；
h） 自主访问控制应能与身份鉴别和审计相结合，记录用户的各种行为；
i） 客体拥有者应是唯一能够修改该客体访问权限的主体；
j） 客体拥有者的控制权不允许分配给其他主体。

7.3.2 强制访问控制

网络产品操作系统内核应提供如下强制访问控制机制：
a） 应采用标记的方法为系统所有主体和客体（包括系统所有的进程、文件、目录等）标明其安全属性；
b） 应基于标记和安全策略模型，实现主体对客体读、写和执行等操作的访问控制；
c） 应与用户身份鉴别、标记等安全功能紧密结合，包含但不限于：
1） 系统对用户的安全控制包含从系统启动到退出系统的全过程；
2） 强制访问控制对客体的控制范围涉及操作系统内部文件或数据的存储、处理和传输过程。
d） 强制访问控制应与审计功能相结合，记录用户的各种行为。

7.3.3 最小权限

网络产品操作系统内核应提供如下最小权限机制：
a） 应仅给主体（如内核服务、用户态驱动、进程等）分配完成其操作所必须的最小的权限；
b） 在未配置权限、不授权、不传递权限的情况下，主体应默认不具备任何权限；
c） 创建用户时，应设置分组，并为每个用户和组分配最小控制权限，如读和执行权限，避免高权限带来的风险；
d） 应设置强制访问控制机制，限制进程和用户的授权范围，防止提升权限和越权访问。

7.4 存储安全要求

7.4.1 持久化数据存储安全

网络产品操作系统内核提供的持久化数据存储应满足以下安全要求：
a） 应支持磁盘加密能力；
b） 支持盘级加密或文件级加密时，应为不同的盘、卷、文件提供不同的加密密钥；
c） 应提供文件加密服务，允许用户对指定的文件和目录进行单独加密；
d） 文件加密密钥应满足7.6小节中的要求；
e） 应提供数据完整性保护机制，在访问数据时进行完整性检查；
f） 应提供文件系统和磁盘的完整性检查功能；
g） 应具备对文件系统操作的安全审计机制；
h） 应使用访问控制机制限制对文件系统的访问途径和方式。

7.4.2 易失性数据存储安全

网络产品操作系统内核提供的易失性数据存储应满足以下安全要求：

a) 应支持内存中数据加密机制，避免通过直接物理内存、重映射、冷启动等方式获取内存中的敏感数据；
b) 应增加敏感数据在内存中地址的随机性；
c) 应支持在数据使用前对内存数据进行初始化和安全检查；
d) 内存资源被回收或再分配时，应保证其中所留存的信息不可用或清除其中留存的信息。

7.5 通信安全要求

7.5.1 通用要求

网络产品操作系统内核应在提供的用户态通信机制、系统模块通信机制、用户态与内核通信机制、对外通信机制中满足以下通用安全要求：

a) 应提供传输数据的完整性保护；
b) 应提供传输数据的机密性保护；
c) 应提供通信双方的身份认证机制，以保障安全通信通道的建立。

7.5.2 用户态通信特殊要求

网络产品操作系统内核在提供用户态通信机制时，除了满足7.5.1的通用要求外，减少用户态进程可调用的通信接口，以减少用户态和内核态的攻击面。

注：用户态通信主要指用户态中不同部分代码的通信机制，如进程间通信机制，常见的有共享内存、队列、信号量、binder等。

7.5.3 系统模块间通信安全

网络产品操作系统内核提供的用户系统模块间通信机制应满足7.5.1的通用要求。

7.5.4 用户态进程与内核通信安全

网络产品操作系统内核提供的用户态进程与内核通信机制应满足7.5.1的通用要求。

7.5.5 对外通信安全

网络产品操作系统内核提供的对外通信机制除了应满足7.5.1的通用要求之外，还应满足以下安全要求：

a) 应对网络模块接口进行权限管控，只有被授权的进程才能访问网络；
b) 应提供数据交换中参与方防抵赖机制。

7.6 密码安全要求

7.6.1 密钥管理

网络产品操作系统内核密钥管理要求包含但不限于：

a) 应支持硬件可信芯片作为信任根；
b) 应支持使用硬件可信芯片作为随机数生成器；
c) 应对密钥提供基于硬件信任根的可信存储支持；
d) 应提供标准化的密钥管理机制用以生成、分发、存储、更新和撤销加密密钥、证书，以确保密钥、证书的安全性和完整性，且该机制应提供系统调用供用户态程序管理密钥、证书；
e) 密钥管理机制应加密保护被管理的密钥、证书，防止密钥、证书被窃取；

f） 密钥管理机制应使用硬件信任根的可信存储保护根密钥；
g） 密钥管理机制应具备访问控制功能，以限制对密钥、证书的访问。

7.6.2 加密算法

网络产品操作系统内核提供的对称、非对称、哈希等算法不应为已被破解的算法。

7.7 自保护要求

7.7.1 入侵检测

网络产品操作系统内核应支持以下入侵检测能力：
a） 应在系统服务入口点进行业务监控，对内核态信息进行收集和分析；
b） 应支持自定义监控信息，并基于此进行攻击检查；
c） 应对系统服务信息进行收集和分析，识别出基础的异常状态或异常动作。

7.7.2 漏洞防利用

网络产品操作系统内核应支持以下漏洞防利用机制：
a） 应支持数据段不可执行机制；
b） 应支持可写内存不可执行机制；
c） 应支持可执行内存不可读机制；
d） 应采用Stack Canary等机制对栈进行保护；
e） 应支持地址空间布局随机化（ASLR）机制；
f） 应支持内核镜像加载时的物理地址随机化。

7.7.3 保持安全状态

当发生故障时，操作系统内核应保持安全状态，例如：不泄露敏感数据。

7.8 日志审计要求

7.8.1 日志生成

网络产品操作系统内核应具备以下日志生成能力：
a） 网络产品操作系统内核应至少为以下可审计事件生成日志记录：
1） 身份鉴别成功或失败；
2） 访问授权成功或失败；
3） 异常访问，例如未授权的访问、异常访问模式等；
4） 应用程序错误或系统事件，例如语法和运行时错误、文件系统错误、配置错误、系统崩溃、内核错误等；
5） 系统配置更改，包括对系统参数、安全策略、防火墙规则等的修改；
6） 应用程序和系统启动、关闭、重启、初始化；
7） 使用高风险功能，例如网络连接、添加或删除用户、权限修改、给令牌添加用户、添加或删除令牌、使用系统管理员权限、应用程序管理员访问、具有管理员权限的用户的行为、创建和删除系统级对象、数据导入导出。
b） 生成的日志记录应至少包含以下信息：
1） 日志的日期和时间；
2） 事件的日期和时间；

3） 事件涉及主客体标识；
4） 事件类型；
5） 事件结果。

c） 生成的日志记录不应包含以下信息：
1） 以明文形式存在的敏感信息，如用户口令、加密密钥、访问令牌、API令牌、数据库链接字符串等；
2） 非开源的源代码；
3） 需要用户同意而未获同意的信息。

7.8.2 日志分析

网络产品操作系统内核应具备以下日志分析能力：

a） 应支持异常行为检测，如未授权访问、异常登录、系统资源滥用的检测等；
b） 应支持安全策略设置和调整，如设置检测规则、根据异常行为检测结果调整用户权限、访问控制策略和审计策略等。

7.8.3 日志存储

网络产品操作系统内核提供的日志存储应满足以下要求：

a） 应为存储区域或设备提供访问控制机制，防止未经授权的访问和破坏日志记录；
b） 应限制对日志的访问权限，普通用户只能产生日志，不应有读取、修改、删除日志的权限；
c） 应内置篡改检测机制，及时检测或者阻止日志记录被非法修改、删除；
d） 应对日志数据进行加密存储；
e） 当超出磁盘存储空间阈值时，应采取措施防止数据丢失，如覆盖旧的日志记录等；
f） 应提供日志记录的定期备份功能。

7.8.4 可信时间戳

网络产品操作系统内核日志审计功能使用的时间戳要求如下：

a） 应为日志审计功能提供时间戳，在生成日志时，应将日志内容与权威时间一起进行存储或传输；
b） 日志记录所使用的时间戳应为本地可信时间源所产生的时间。

附 录 A
（规范性）
安全等级划分

本文件中三个安全等级对应的条款见表 A.1。

表 A.1 网络产品操作系统内核安全技术要求条款等级划分表

安全要求	一级	二级	三级
完整性保护要求	7.1.1	7.1.1	7.1.1
	7.1.2a)	7.1.2a)	7.1.2a)
	--	7.1.2b)	7.1.2b)
	--	7.1.3a)	7.1.3a)
	--	7.1.3b)	7.1.3b)
	--	7.1.3c)	7.1.3c)
	--	7.1.3d)	7.1.3d)
	--	--	7.1.3e)
	--	--	7.1.3f)
	--	--	7.1.4
隔离要求	7.2.1	7.2.1	7.2.1
	--	7.2.2	7.2.2
	--	7.2.3	7.2.3
	--	--	7.2.4
	--	--	7.2.5
	--	--	7.2.6
访问控制要求	7.3.1a)	7.3.1a)	7.3.1a)
	7.3.1b)	7.3.1b)	7.3.1b)
	7.3.1c)	7.3.1c)	7.3.1c)
	--	7.3.1d)	7.3.1d)
	--	7.3.1e)	7.3.1e)
	--	7.3.1f)	7.3.1f)
	7.3.1g)	7.3.1g)	7.3.1g)
	7.3.1h)	7.3.1h)	7.3.1h)
	7.3.1i)	7.3.1i)	7.3.1i)
	7.3.1j)	7.3.1j)	7.3.1j)
	--	7.3.2	7.3.2
	--	7.3.3	7.3.3
存储安全要求	--	7.4.1	7.4.1
	--	7.4.2	7.4.2
通信安全要求	7.5.1	7.5.1	7.5.1
	--	7.5.2	7.5.2
	7.5.3	7.5.3	7.5.3

表 A.1　网络产品操作系统内核安全技术要求条款等级划分表（续）

安全要求	一级	二级	三级
通信安全要求	7.5.4	7.5.4	7.5.4
	--	7.5.5	7.5.5
密码安全要求	--	--	7.6.1
	7.6.2	7.6.2	7.6.2
自保护要求	--	7.7.1	7.7.1
	--	--	7.7.2
	7.7.3	7.7.3	7.7.3
日志审计要求	7.8.1	7.8.1	7.8.1
	7.8.2	7.8.2	7.8.2
	7.8.3	7.8.3	7.8.3
	--	7.8.4	7.8.4

附 录 B
（资料性）
安全风险分析

B.1 安全资产

网络产品操作系统内核需要保护的核心资产如下：

a） 系统配置数据，如安全启动验签密钥；
b） 存储的代码包；
c） 系统审计日志数据；
d） 内核服务进程运行产生的数据；
e） 系统用户产生、存储的数据；
f） 运行中的代码和进程。

网络产品操作系统内核在设计和研发过程中应采取措施保护上述资产的机密性、完整性和可用性。

B.2 安全风险

网络产品操作系统内核可能面临以下安全风险：

a） 系统完整性破坏：
   1） 攻击者通过替换或篡改内核可执行文件或其升级包，注入恶意代码加载运行；
   2） 攻击者通过篡改进程读取的数据，注入恶意数据；
   3） 攻击者通过篡改进程数据流和控制流，实施恶意行为。
b） 非授权访问：
   1） 隔离机制设计不严谨，导致攻击者突破不同区域的边界访问其不应访问的内容，例如用户态中的攻击者进程访问内核态中的资源；
   2） 访问控制机制设计不严谨，被攻击者利用，滥用权限或越权访问资源。
c） 存储数据被泄露、篡改、替换：
   1） 持久化存储数据未进行安全保护，导致攻击者可以获取敏感数据、篡改或替换关键配置数据，如替换安全启动验签密钥；
   2） 内存中的易失性数据未进行安全保护，导致攻击者可以从内存中抓取敏感数据、篡改或替换进程输入数据，实施恶意行为。
d） 传输数据被泄露、篡改、替换：
   1） 攻击者通过侦听不同主体间（如用户态进程间、系统模块间、内核与外部间）的通信，截获其中传输的机密数据；
   2） 攻击者修改不同主体间的通信数据，触发数据接收方的敏感操作或导致其功能异常。
e） 内核功能可用性破坏：
   1） 攻击者通过构造堆栈溢出场景改变目标代码的运行逻辑；
   2） 攻击者触发系统故障导致整个内核功能丧失。

参 考 文 献

[1] GB/T 20272-2019 信息安全技术 操作系统安全技术要求
[2] GB/T 30284-2020 信息安全技术 移动通信智能终端操作系统安全技术要求
[3] GB/T 36630.3-2018 信息安全技术 信息技术产品安全可控评价指标 第3部分：操作系统
[4] GB/T 39276-2020 信息安全技术 网络产品和服务安全通用要求

电信终端产业协会团体标准

网络产品操作系统内核安全技术要求

T/TAF 249—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn