电 信 终 端 产 业 协 会 标 准

TAF-WG9-AS0038-V1.0.0:2019

网络关键设备安全技术要求
交换机设备

Security Techniques Requirement for Critical Network Devices: Switch

2019－07－24 发布　　2019－07－24 实施

电信终端产业协会　　发 布

目　次

前　言

TAF-WG9-AS0038-V1.0.0:2019《网络关键设备安全技术要求 交换机设备》与TAF-WG9-AS0029-V1.0.0:2018《网络关键设备安全技术要求 通用要求》、TAF-WG9-AS0039-V1.0.0:2019《网络关键设备安全技术要求 路由器设备》等共同构成支撑网络关键设备安全检测工作的系列团体标准。

本标准对交换机设备提出安全技术要求。对列入网络关键设备目录的交换机，除满足本标准要求，还应满足TAF-WG9-AS0029-V1.0.0:2018《网络关键设备安全技术要求 通用要求》。

本标准/本部分由电信终端产业协会（TAF）提出并归口。

本标准起草单位：中国信息通信研究院、新华三技术有限公司、华为技术有限公司、烽火通信科技股份有限公司、北京启明星辰信息安全技术有限公司、中兴通讯股份有限公司、杭州迪普科技股份有限公司、联想（北京）有限公司、浪潮思科网络科技有限公司。

本标准主要起草人：张治兵、倪平、童天予、祝东健、陈鹏、叶郁柏、邓科、蒋鹏、苏燕谨、许雯、杨达、仇俊杰、徐强 、过育红、邵红波、张仲凯、刘文德。

引　　言

按照《中华人民共和国网络安全法》（以下称《网络安全法》）有关要求，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，对列入目录的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

本规范对交换机设备提出安全技术要求。对列入网络关键设备目录的交换机，除满足本标准要求，还应满足TAF-WG9-AS0029-V1.0.0:2018《网络关键设备安全技术要求 通用要求》。

网络关键设备安全技术要求 交换机设备

1 范围

本标准对列入网络关键设备的交换机设备在标识安全、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、数据安全等方面提出了安全技术要求。

本标准适用于在我国境内销售或提供的交换机设备，也可为网络运营者采购交换机设备时提供依据，还适用于指导交换机设备的研发、测试等工作。

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，仅所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 25069-2010 信息安全技术 术语

TAF-WG9-AS0029-V1.0.0:2018 网络关键设备安全技术要求 通用要求

3 术语和定义

GB/T 25069-2010中界定的以及下列术语和定义适用于本文件。

3.1 交换机 switch

在联网的设备之间，一种借助内部交换机制来提供连通性的设备。交换机不同于其他局域网互联设备（例如集线器），交换机中使用的技术是以点对点为基础建立连接，这确保了网络通信量只有对有地址的网络设备可见，并使几个连接能够并存。交换技术可在开放系统互联参考模型的第二层或第三层实现。

3.2 恶意程序 malware

一种企图通过执行非授权过程来破坏信息系统机密性、完整性和可用性的软件或固件。常见的恶意程序包括病毒、蠕虫、木马或其它影响设备安全的程序代码。恶意程序也包括间谍软件和广告软件。

3.3 预装软件 preset software

设备出厂时安装的软件和正常使用必须的配套软件，包括固件、系统软件、应用软件、配套的管理软件等。

3.4 故障隔离 fault isolation

相互独立的硬件模块或者部件之间，任一模块或部件出现故障，不影响其他模块或部件的正常工作。

4 安全技术要求

4.1 标识安全

交换机设备：

a) 硬件整机和主控板卡、业务板卡等主要部件应具备唯一性标识；
b) 应对软件/固件、补丁包/升级包的版本进行唯一性标识，并保持记录；
c) 应标识每一个物理接口，并说明其功能，不得预留未向用户声明的物理接口；
d) 在用户登录通过认证前的提示信息应避免包含设备软件版本、型号等敏感信息，例如可通过支持关闭提示信息或者用户自定义等功能实现。

4.2 可用性

交换机设备：

a) 部分关键部件，如主控板卡、交换网板、电源、风扇等应支持冗余功能，在设备运行状态异常可能影响网络安全时，可通过启用备用部件防范安全风险；
b) 部分关键部件，如主控板卡、交换网板、业务板卡、电源、风扇等应支持热插拔功能；
c) 软件/固件、配置文件等应支持备份与恢复功能；
d) 支持故障的告警、定位等功能；
e) 支持部分关键部件，如主控板卡、交换网板、业务板卡、电源、风扇等故障隔离功能；
f) 应提供独立的管理接口，实现设备管理和数据转发的隔离。

4.3 漏洞与缺陷管理安全

交换机设备：

a) 部分关键部件，如 CPU、系统软件的存储部件等应不存在已知的高危和中危漏洞或具备有效措施防范硬件漏洞安全风险；
b) 预装软件应不存在已公布的高危和中危漏洞或具备有效措施防范漏洞安全风险；
c) 第三方组件或部件存在暂未修复的已知漏洞或安全缺陷时，应明确告知用户风险及防范措施；
d) 预装软件、补丁包/升级包应不包含恶意程序；
e) 应不存在未向用户声明的功能和隐蔽通道。

4.4 软件更新安全

交换机设备：

a) 对于更新操作，应仅限于授权用户可实施，应不支持自动更新；
b) 对于存在导致设备重启等影响设备运行安全的实施更新操作应由用户确认后实施；
c) 应支持用户对软件版本降级使用；
d) 应支持软件更新包完整性校验；
e) 应支持软件更新包签名机制，抗抵赖攻击，签名应使用安全性较高的算法，如 SHA256，避免使用 MD5 等安全性较差的算法；
f) 更新失败时设备应能够恢复到升级前的正常工作状态；
g) 对于采用远程更新的，应支持非明文通道传输更新数据；
h) 应具备稳定可用的渠道提供软件更新源。

4.5 默认状态安全

交换机设备：

a) 出厂应预装满足功能需求且安全风险较低的软件版本；
b) 出厂默认开放的端口和服务应明示用户，满足最小够用原则；
c) 使用 Telnet、SNMPv1/v2c、HTTP 等明文传输协议的网络管理功能应默认关闭；
d) 对于存在较多版本的远程管理协议，应默认关闭安全性较低的版本，例如设备支持 SSH 协议时，应默认关闭 SSHv1。

4.6 抵御常见攻击能力

交换机设备：

a) 应具备抵御目的为交换机自身的大流量攻击的能力，例如目的为交换机管理接口的 ICMPv4/v6 Ping request Flood 攻击、TCPv4/v6 SYN Flood 攻击等；
b) 应支持防范 ARP/ND 欺骗攻击功能，如通过 MAC 地址绑定等功能实现；
c) 应支持开启生成树协议等功能，防范广播风暴攻击；支持关闭生成树协议，或支持启用 Root Guard、BPDU Guard 等功能，防范针对生成树协议的攻击；
d) 应支持连续的非法登录尝试次数限制或其他安全策略，以防范用户凭证猜解攻击；
e) 应支持限制用户会话连接的数量，以防范资源消耗类拒绝服务攻击；
f) 在支持 WEB 管理功能时，应具备抵御常见 WEB 攻击的能力，例如注入攻击、重放攻击、权限绕过攻击、非法文件上传等；
g) 在支持 SNMP 管理功能时，应具备抵御常见攻击的能力，例如权限绕过、信息泄露等；
h) 在支持 SSH 管理功能时，应具备抵御常见攻击的能力，例如权限绕过、拒绝服务攻击等；
i) 在支持 Telnet 管理功能时，应具备抵御常见攻击的能力，例如权限绕过、拒绝服务攻击等；
j) 在支持 RestAPI 管理功能时，应具备抵御常见攻击的能力，例如 API 身份验证绕过攻击、HTTP 身份绕过攻击、Oauth 绕过攻击、拒绝服务攻击等；
k) 在支持 NETCONF 管理功能时，应具备抵御常见攻击的能力，例如权限绕过、拒绝服务攻击等；
l) 在支持 FTP 功能时，应具备抵御常见攻击的能力，例如目录遍历、权限绕过等。

4.7 身份标识与鉴别

交换机设备：

a) 应不存在未向用户公开的身份鉴别信息；
b) 应对访问控制主体进行身份标识和鉴别；
c) 用户身份标识应具有唯一性；
d) 应支持登录用户空闲超时锁定或自动退出等安全策略，以防范会话空闲时间过长导致的安全风险；
e) 对身份鉴别信息，如用户登录口令、SNMP 团体名等应使用安全强度较高的密码算法，如 AES、SM3/4、SHA2 等，来保障身份鉴别信息存储的机密性，避免使用 base64、DES、SHA1 等安全强度弱的密码算法；
f) 对于使用口令鉴别方式的设备，用户首次管理设备时，应提示并允许用户修改默认口令或设置口令；

g） 应支持设置口令修改周期；
h） 对于使用口令鉴别方式的设备，应默认开启口令复杂度检查功能。开启口令复杂度检查功能时，口令长度应不少于 8 位，且至少包含 2 种不同类型字符；
i） 用户输入的用户登录口令、SNMP 团体名等鉴别信息默认应是不可见的；
j） 鉴别失败时，设备应返回最少且无差别信息。

4.8 访问控制安全

交换机设备：
a） 应在出厂时默认设置安全的访问控制策略，或支持用户首次使用时设置访问控制策略；
b） 应提供用户分级分权控制机制；
c） 对涉及设备安全的重要功能如补丁管理、固件管理、日志审计、时间同步、端口镜像、流采样等，应仅高等级权限用户可使用；
d） 应支持对用户管理会话进行过滤，限制非授权用户访问和配置设备，例如通过访问控制列表功能限制可对设备进行管理（包括 Telnet、SSH、SNMP、WEB 等管理方式）的用户 IPv4/v6 地址。

4.9 日志审计安全

交换机设备：
a） 应提供日志记录功能，对用户关键操作，如增/删账户、修改鉴别信息、修改关键配置、开启/关闭日志记录、用户登录/注销、用户权限修改、重启/关闭设备、更新等行为进行记录；对常见攻击行为例如 SYN Flood、ICMP Flood、UDP Flood、IP Flood、IP 地址扫描、端口扫描、Ping of Death、TearDrop、IP 选项伪造、TCP 异常、Smurf、Fraggle、Land 等攻击行为进行记录；
b） 应提供日志信息本地存储功能，当日志记录存储达到极限时，应采取覆盖旧的审计记录，保留最新的审计记录等措施；
c） 应支持日志信息输出功能；
d） 应提供安全功能，保证设备异常断电恢复后，已记录的日志不丢失；
e） 日志审计记录中应记录必要的日志要素，至少包括事件发生日期和时间、主体、事件描述（如类型、操作结果等）、IP 地址（采用远程管理方式时）等，为查阅和分析提供足够的信息；
f） 应提供日志分析功能或为日志分析功能提供接口；
g） 日志记录应受到保护，防止日志内容被修改，防止未经授权的操作；
h） 不应在日志中明文记录敏感信息，如用户口令、SNMP 团体名、WEB 会话 ID 以及私钥等。

4.10 通信安全

交换机设备：
a） 管理系统（管理用户）与设备之间的通信信道/路径应保证数据的机密性和完整性；
b） 在支持 WEB 管理时，应支持 HTTPS；
c） 在支持 SSH 管理时，应支持 SSHv2；
d） 在支持 SNMP 管理时，应支持 SNMPv3；
e） 应支持使用至少一种非明文数据传输协议对设备进行管理，如 HTTPS、SSHv2、SNMPv3 等；
f） 应支持关闭网络管理功能，如 Telnet、SSH、SNMP、WEB 等网络管理功能；
g） IPv4/v6、TCP、UDP、ICMPv4/v6 等基础通信协议应满足一定的通信协议健壮性要求，防范异常报文攻击；

h） SNMPv1/v2c/v3、SSHv1/v2、HTTP/HTTPS、FTP、TFTP、NTP、netconf、Openflow 等应用层协议应满足一定的通信协议健壮性要求，防范异常报文攻击；
i） 如果支持路由功能，则 OSPFv2/v3、BGP4/4+等路由控制协议应满足一定的通信协议健壮性要求，防范异常报文攻击；
j） 如果支持路由功能，则路由通信协议应支持非明文路由认证功能，例如基于 MD5 的路由认证；
k） 应支持使用 NTP 等实现时间同步功能，并具备安全功能或措施防范针对时间同步功能的攻击，如提供 NTP 认证等功能；
l） 如果支持 TRILL 协议，应支持协议认证功能，如基于 HMAC-SHA256 等认证。

4.11 数据安全

交换机设备：

a） 应对存储在设备上的数据进行分类管理，如对用户口令等敏感数据具备安全防护措施；
b） 设备提供者通过设备收集用户信息功能的，应当向用户明示并取得同意。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容
2018-10-18	V1.0.0	标准征求意见稿初稿
2018-11-7	V1.0.1	根据各厂商意见，修订标准，形成征求意见稿
2019-1-10	V1.1.0	根据各厂商意见，修订标准，形成送审稿
2019-4-10	V1.2.0	根据各厂商意见，修订标准，形成报批稿

附 录 B
（资料性附录）
用户信息说明

对于网络关键设备而言，用户可能是运营商、大中型企业等组织。其所涉及的用户信息，可能包括路由表、设备及软件配置信息、设备运行日志等信息。

参 考 文 献

1） ITU-T X.805 端到端通信服务安全框架
2） GB/T 18336-2015 信息技术 安全技术 信息技术安全性评估准则
3） YD/T 1629-2007 具有路由功能的以太网交换机设备安全技术要求
4） YD/T 1630-2007 具有路由功能的以太网交换机设备安全测试方法
5） YD/T 2042-2009 IPv6 网络设备安全技术要求——具有路由功能的以太网交换机
6） YD/T 2043-2009 IPv6 网络设备安全测试方法——具有路由功能的以太网交换机
7） GB/T 21050-2007 信息安全技术 网络交换机安全技术要求（评估保证级 3）