附件

“两高一弱”问题自查指南

一、“两高一弱”问题专项整治范围

(一) 高危漏洞。高危漏洞指存在严重安全风险的软件、系统或组件漏洞，包括但不限于远程代码执行、数据泄露、拒绝服务、提权攻击、跨站脚本攻击等漏洞，经常被攻击者攻击利用，

(二) 高危端口。高危端口指对外开放暴露，因缺乏访问控制措施或存在高危漏洞、弱口令等问题，能够轻易被攻击者利用以的端口，常见高危端口包括数据库、FTP、远程桌面、共享服务等类型，

(三) 弱口令。弱口令是指复杂性低、规律性强、系统默认等轻易被黑客猜解的密码，例如口令大批量复用、键盘临近组合、姓名拼音等。

二、排查范围

（一）资产范围。应覆盖互联网侧和内网侧（包括办公网、业务内网、生产网），具体资产包括：一是网络基础设施。包括运行 Web 应用、邮件服务、网络安全服务及数据库的服务器，路由器、交换机、防火墙等网络设备，云服务器、云数据库等企业云资源以及移动终端、办公主机等各类终端设备；二是重要网络系统。涵盖办公系统、移动应用、运维管理系统、堡垒机及对外提供服务的 API 接口；三是数据信息资产。如企业域名、IP

地址、邮箱账号等基础数据标识。此外，从系统防护层面，需重点关注数据库系统、堡垒机等高交互核心系统，此类系统因权限集中、数据敏感，历来是攻击者的重点目标。

（二）管理范围。一是地域层级。包括总公司、所有分支机构的自建或租赁的数据中心、远程办公节点以及临时搭建的网络接入环境等。二是合作方范围。包括具有数据交互或系统直连权限的核心供应链企业、运维及软件开发外包服务商以及基础设施托管方等。

三、排查方式

针对“两高一弱”的排查，需建立“常态化、动态性、滚动式”的动态防控机制，具体实施如下：一是工具自动化测绘。通过资产测绘工具对全网资产实施周期性扫描，动态识别开放端口、服务指纹及漏洞特征（如进行 CVE、CNVD 漏洞库匹配）。二是人员权限治理与弱口令专项清查。强化运维、安全人员密码本安全管理并禁用明文存储；专项排查开发测试环境的默认账户、公共服务组件弱口令等，并及时清理离职未回收账户；对外包团队临时账户设置访问时效和权限围栏，确保“用后即焚”；利用脚本批量验证弱口令，结合人工复核查验，形成问题清单并限期整改。三是构建资产归属闭环与滚动更新机制。明确每项资产（包括云资源、第三方组件）的业务归属、部署位置及责任人，形成发现、修复、复验、优化的闭环管理，杜绝风险滞留。

四、整改原则与建议

各单位按照“发现一个、整改一个”的原则，对发现的“两高一弱”问题举一反三，动态治理。

（一）高危漏洞防护建议。一是强化主机防护，开展系统层和应用层加固。二是监测网络外联访问行为。防止漏洞利用被植入木马后门。三是加强网络威胁情报共享，及时修补漏洞隐患，阻断攻击入侵。四是动态性、周期性开展网络资产摸底，发现、处置存在高危漏洞的风险资产。五是加强对开源软件组件、通用性软硬件风险排查，做好举一反三、全面加固。六是与供应链企业加强紧密联系，及时掌握漏洞补丁更新升级情况。七是优化数据库、中间件、网络设备等规则配置，避免出现防护缺陷和逻辑漏洞。八是优化升级应用防火墙（WAF）、流量检测等安全防护设备规则库，拦截高危漏洞利用等网络攻击行为。

（二）高危端口防护建议。一是最小化端口开放。仅开放业务必须的端口，关闭不必要的端口以减少攻击面。二是优化防火墙策略。强化对必要端口的访问权限控制，仅允许受信任的 IP 地址访问关键端口。三是限制服务默认端口使用。在部署服务时，尽量使用自定义端口代替默认端口。注意关闭一些服务、框架和组件默认开启的端口，以减少服务信息暴露。四是建立端口服务管理机制。建立端口和服务关联关系台账、严禁端口使用未申请的服务；端口开放前需进行安全审批，并留存对应的变更审计日志。五是多重验证。对远程访问和敏感端口实施多因素认证，防止未经授权的访问。六是网络分段和微分区。将网络分置为不同

区域，将重要的系统放在单独的区域内，限制高危端口的暴露范围，防止攻击行为扩散至网络多个部分。七是建立监控防御机制。通过扫描测绘和内部审计，持续监控发现对外暴露的高危端口并第一时间进行处置；通过流量监控识别通过高危端口的恶意攻击流量，部署入侵防御系统及时进行攻击阻断。八是日志记录与审计。对端口访问进行详细日志记录，定期审计以发现和应对潜在威胁。九是探索应用反测绘等技术，隐藏或混淆端口服务信息，提高攻击者测绘和扫描成本。十是使用安全协议在充分评估系统兼容性，性能需求、安全要求、成本和法规要求等实际需求和环境条件的前提下，选择使用安全协议替代不安全协议，确保替代后既提升安全性，又不会给系统带来不必要的负担。常见的替代方案有采用 SSH 替代 Telnet、HTTPS 替代 HTTP、FTPS/SFTP 替代 FTP、SMTPS 替代 SMTP、WebSockets over TLS（WSS）替代 WebSockets 等。

（三）弱口令防护建议。一是设定密码长度、复杂度和历史密码策略，如密码长度不得少于 8 位，必须包含大小写字母、数字和特殊字符，且不能与最近使用的密码相同。二是强制用户定期更换密码，并限制密码更换的间隔时间。三是禁止用户将密码设置常见词汇、用户名、生日等易于猜测的内容。四是鼓励用户为不同的系统和应用设置不同的密码，避免使用同一密码。五是开启多因素认证，并对涉及用户认证的功能模块，启用验证码、限制 IP 登录频次等防御暴力破解机制。六是限制登录尝试次数。

设置尝试登录失败的次数限制，超过限制后暂时锁定账户或延长下次尝试的时间。七是实施账户审计和监控。定期审计账户的密码使用情况，及时发现和纠正使用弱口令的行为，监控异常登录活动，如异地登录、非常规时间登录等，及时响应可疑行为。