网络安全漏洞防范应对指南

国家计算机网络应急技术处理协调中心

2022 年 9 月

目录

一、编写目的

为防范和应对网络安全漏洞风险，增强关键信息基础设施应对网络安全漏洞的能力，指导相关单位科学开展事前防范、事中处置和事后恢复，特制定本指南。

二、网络安全漏洞的定义与危害

（一）网络安全漏洞定义

安全漏洞是指信息系统在生命周期的各个阶段（设计、实现、运维等过程）中产生的某类问题，这类问题会对系统的安全（机密性、完整性、可用性）产生影响。如果漏洞造成敏感信息泄露，就会导致系统的机密性被破坏；如果使数据库中的信息被非法篡改，就会导致系统的完整性被破坏；如果使服务器的进程崩溃，那么就导致系统可用性的丧失。有些漏洞也可能同时导致多个安全属性的破坏。

（二）网络安全漏洞危害

漏洞危害程度用来描述漏洞被成功触发后，对受影响实体造成的影响情况。漏洞危害程度可以从机密性、完整性和可用性等三个维度受影响的程度进行描述，每个程度的取值范围包括：高、低和无。机密性用来衡量漏洞在成功利用后，对受影响实体（如：系统、模块、软硬件等）使用或管理数据（例如信息、文件）的机密性影响程度。完整性用来衡量漏洞在成功利用后，对受影响实体的完整性影响程度。可用性用来衡量漏洞在成功利用后，对受影响实体的可用性影响

程度。攻击者对网络带宽资源、计算资源或者存储资源的攻击均会对受影响实体的可用性构成一定的影响。

（三）漏洞易发的位置

1.Web 应用层

主要是各类 B/S 架构的业务应用自身由于开发过程中未遵循安全开发规范而产生的各类安全漏洞，如 SQL 注入漏洞、XSS 跨站脚本攻击漏洞等，这些漏洞与承载业务应用的操作系统、数据库、中间件无关。

2.系统层

主要是承载业务应用的操作系统、数据库、中间件以及各类用于业务应用开发的应用组件自身存在的安全漏洞。

3.系统配置层

作为 IT 信息系统脆弱性的一个表现形式，安全配置方面的缺陷也会引入安全风险，使得攻击者可以绕过系统的安全防护，例如账号没有开启多次错误尝试锁定策略，则将会面临口令被暴力破解的风险。因此，应将安全配置方面的问题，也列为常态化安全漏洞检测的一个方面；

4.登录认证口令

很多组织的 IT 系统操作人员和维护人员缺乏安全意识，为了方便日常记忆，关键业务应用、系统设备等的账号都会设置为相对简单的口令，且长时间不去更换。这些弱口令被利用后可以轻松绕过系统的安全防护机制，因此占众多安全

事件发生原因的很大一部分，也需要作为一个漏洞方面提起重视。

（四）常见的网络安全漏洞分类

基于漏洞产生或触发的技术原因可对漏洞类型进行的划分，常见的具体分类如下:

1.缓冲区错误漏洞

缓冲区错误漏洞是指在内存上执行操作时，因缺少正确的边界数据验证，导致在其向关联的其他内存位置上执行了错误的读写操作，如缓冲区溢出、堆溢出等。

2.跨站脚本漏洞

此类漏洞是指在WEB应用中，因缺少对客户端数据的正确验证，导致向其他客户端提供错误执行代码的漏洞。

3.注入漏洞

注入漏洞包括多种类型:

（1）操作系统命令注入漏洞，在构造操作系统可执行命令过程中，因未正确过滤其中的特殊字符、命令等，导致生成了错误的操作系统执行命令;

（2）参数注入漏洞，在构造命令参数过程中，因未正确过滤参数中的特殊字符，导致生成了错误的执行命令;

（3）代码注入漏洞，在通过外部输入数据构造代码段的过程中，因未正确过滤其中的特殊元素，导致生成了错误的代码段，修改了网络系统或组件的预期的执行控制流;

（4）SQL 注入漏洞，在基于数据库的应用中，因缺少对构成 SQL 语句的外部输入数据的验证，导致生成并执行了错误的 SQL 语句。

4. 路径遍历漏洞

路径遍历漏洞是指因未能正确地过滤资源或文件路径中的特殊元素，导致访问受限目录之外的位置。

5. 跨站请求伪造漏洞

跨站请求伪造漏洞是指在 WEB 应用中，因未充分验证请求是否来自可信用户，导致受欺骗的客户端向服务器发送非预期的请求。

6. 信任管理漏洞

此类漏洞是因缺乏有效的信任管理机制，导致受影响组件存在可被攻击者利用的默认密码或者硬编码密码、硬编码证书等问题

7. 权限许可和访问控制漏洞

权限许可和访问控制漏洞是指因缺乏有效的权限许可和访问控制措施而导致的安全问题。

8. 默认配置错误漏洞

默认配置错误漏洞，因默认不安全的配置状态而产生的漏洞。

9. 信息泄露漏洞

信息泄露漏洞是指在运行过程中，因配置等错误导致的

受影响组件信息被非授权获取的漏洞，包括日志信息泄露漏洞，因日志文件非正常输出导致的信息泄露；调试信息泄露漏洞，在运行过程中因调试信息输出导致的信息泄露。

三、漏洞信息获取与威胁发现

（一）定期开展漏洞排查工作

积极利用自动化安全漏洞检测工具，建立常态化的安全漏洞排查机制，在组织内部定期进行全面的漏洞排查工作，并将发现的安全漏洞及时进行处置，形成漏洞发现到处置到再发现再处置的良性循环，使业务系统受安全漏洞影响的风险始终处于可管可控的程度。

（二）借助外部力量开展漏洞检测

关注互联网各类网络安全信息发布渠道或安全厂商信息发布平台，或者与有能力的安全厂商直接合作，利用安全厂商的资源、技术能力优势，在全面掌握组织自身资产情况的前提下，随时根据最新的安全漏洞情报，评估自身系统资产的受影响情况。针对重要性程度较高的业务系统，可以在工具检测的基础上，进一步聘请第三方专业机构或采用安全众测的机制，引入人工专家安全测试，确保深入全面的安全漏洞检测。

（三）跟踪最新安全漏洞信息

此外，可通过与 CNVD 国家漏洞平台合作，及时获取与组织相关的安全漏洞信息，主动应对漏洞事件，尤其是银行、

证券、保险等强监管行业以及能源、交通、电力、电信等关系国计民生的关键信息基础设施行业组织单位。

四、漏洞应对处置流程

（一）确认漏洞基本情况

1.排查漏洞是否真实存在

（1）版本排查：根据漏洞影响分析得出的影响资产进一步确认产品及服务的版本。

（2）中间件排查：组件通常会嵌套在其他中间件使用，需要相关人员查看开发文档或联系系统开发商、维护人员进行判断是否有使用相关中间件。

2.排查漏洞是否已经被利用

（1）系统或服务可疑进程分析。使用 PCHunter、Procexp64 等工具对进程、服务、启动项、任务计划进行分析，发现可疑进程。

（2）异常流量分析。根据查看捕获设备流量情况分析是否存在异常流量、外联行为以及下载行为等等。

（3）可疑用户分析。查看服务器是否存在隐藏用户，通过计算机管理或者注册表中查看隐藏用户。

（4）日志分析。分析系统日志、中间件日志和安全设备日志等。日志记录了接收处理请求及运行时错误等各种原始信息。通过对 WEB 日志进行的安全分析，不仅可以帮助我们定位攻击者，还可以帮助我们还原攻击路径，找到网站存

在的安全漏洞并进行修复。

（5）漏洞利用相关 IOC 排查。扫描与利用漏洞相关的已知 IOC，排查是否有中招已披露安全事件情况。若排查到已被利用则需要进一步展开安全事件响应，根据以上排查过程确定安全事件性质，如感染勒索软件、挖矿软件及远控木马等等，再进一步根据事件性质进行下一步的事件应急响应。

（二）开展漏洞风险筛查

漏洞风险复查一般通过自动化工具检测和人工专家渗透测试进行。自动化工具检测具有检测速度快、检测项覆盖广、结果自动验证、检测成本低的特点，缺点是无法对存在关联性的漏洞进行深入分析，检测深度有限。而人工专家渗透测试正相反，测试需要花费较长的时间，成本较高，测试人员会深入系统各个功能模块，对自动化工具无法发现的安全漏洞和关联性问题深入分析，确保深层问题能够被及时发现。

在实际的漏洞排查工作中，一般会将自动化工具检测和人工专家渗透测试相结合，以期在深度和广度方面都得到妥善兼顾。自动化工具测试和人工专家渗透虽然能够实现对安全漏洞的持续性检测，但面对当前层出不穷的安全漏洞，由于缺少对新漏洞的利用细节的掌握，往往难以对最新出现的安全漏洞进行快速反应。此时，我们可以通过安全漏洞情报，第一时间对 IT 系统中可能受该漏洞影响的 IT 资产进行快速

评估，通过该漏洞影响的操作系统、数据库、中间件、应用组件的版本进行筛选，匹配出受该漏洞影响的所有资产。

（三）采取紧急处置措施

根据漏洞的威胁程度和严重性，以及对涉事单位的业务的影响程度和范围，可以采取不同的紧急处置措施，包括但不限于：设备紧急下架、虚拟补丁规则下发、收缩安全控制策略等。对于上级指导单位要求紧急修复的漏洞、黑客正在利用的超危，高危漏洞并对涉事单位进行攻击，涉事单位在互联网的业务系统存在的超危、高危漏洞，这三种情况适用于漏洞紧急处置。

设备紧急下架。物理下架方法如下：拔掉设备的网线或禁用网卡，将设备物理隔离在网络中，防止设备被漏洞攻击，待设备上的漏洞被修复完成后，再次将设备连接到网络中。逻辑下架方法如下：将设备的所有访问关系全部关闭，只允许设备访问修复主机，待设备上的漏洞被修复完成后，再次将设备连接到网络中。

虚拟补丁规则下发。虚拟补丁主要是利用主机入侵防护（IPS）过滤规则以及高效能的流量监控能力，可以在网络层侦测到网路流量中的攻击特征，通过在网络层部署攻击特征过滤规则来预防漏洞攻击，可在漏洞补丁未更新之前提供完整的安全防护，有效防御应用层攻击、SQL 注入漏洞及跨站脚本攻击漏洞等，无须重新设备或者操作系统，即可在几

分钟内将虚机补丁下发到成千上万的设备上，对已知和未知漏洞进行安全防护。

安全控制策略收缩。在保障业务的前提下，根据最小访问、最小授权的原则，设置访问控制策略，严格控制用户、进程访问对象的权限。

（四）及时进行漏洞修复

关注漏洞影响产品厂商、安全企业发布的漏洞修复补丁或方案，及时对本单位软硬件设备存在的漏洞进行修复。对于修复周期较长或修复难度较大的，可向软硬件设备厂商或安全企业寻求技术支持。

在漏洞的修复中，需确保流程的严谨性。漏洞修复过程是一项存在业务风险的过程，单位需严格按照漏洞修复的流程完成。针对漏洞进行威胁等级的评估，确定漏洞修复优先级以及修复方案；在测试环境中进行修复测试，择优选取修复方案，确保修复无其他不良影响；正式修复应选在非业务高峰期，修复人员应有运维人员和安全人员共同完成，操作分工明确，并做好详细记录；持续监控并复测漏洞，保障漏洞修复完成。

（五）组织漏洞风险排查

针对影响面广、危害大的重大网络安全漏洞，国家网信部门将组织漏洞影响产品对应的厂商进行复核，并及时发布漏洞修复补丁及方案。对于修复周期较长或修复难度较大的，

可组织相关单位提出临时修复方案。

组织相关单位在全国范围内开展漏洞风险排查工作，探测可能受漏洞影响的网络资产情况，对其进行漏洞检测，以摸清漏洞对我国的整体影响情况，特别是对我国党政机关和关基单位的影响情况。对供应链类型的漏洞，可要求各厂商报送发现的软硬件产品或服务受影响情况，以及产品补丁情况。对发现存在漏洞的情况，要求涉事单位及时开展漏洞修复，并持续跟踪漏洞修复情况。

（六）发布漏洞预警通报

针对影响面广、危害大的重大网络安全漏洞，国家网信部门将通过公众号、工作平台、CNCERT 和 CNVD 的对外网站和微信公众号等渠道，向网信部门、关基单位或社会公开渠道发布漏洞安全公告或征集相关信息，建议各厂商单位对开发的软硬件产品和服务进行积极自查，要求发现存在受漏洞影响情况的立即修复，并通知产品用户及时更新，并将受漏洞影响的产品和服务情况，以及修复措施和补丁情况及时报送至中央网信办。

（七）跟踪漏洞攻击利用情况

国家网信部门组织技术力量对漏洞攻击利用情况开展跟踪监测，获取漏洞利用攻击数据情况，监测发现党政机关等重要行业单位受漏洞影响被攻击、并被利用作为跳板，进一步攻陷单位内部网络等严重网络攻击事件。

重大突发漏洞随着技术原理的进一步研究和衍化，可能会迅速衍生成为其他种类的重大突发攻击事件，包括大规模拒绝服务攻击、大规模僵木蠕爆发传播、域名安全事件、大规模数据泄露、重要网站遭恶意篡改等事件，因此需要在持续跟踪重大漏洞发展的前提下，保持对攻击形态衍化倾向的关注。必要时，需第一时间调集力量、采取相应的技术手段开展应急监测和分析工作。

五、日常防范措施

为缓解漏洞攻击及降低漏洞攻击带来的危害，建议在日常工作中从以下几个方面采取措施加强防范：

（一）及时安装更新补丁或升级系统

由于随着互联网设备或应用的持续运行，网络中会持续不断产生新的漏洞，因此在日常使用过程中应注意及时更新补丁或升级系统，确保自己使用的软硬件产品和服务处于最新版本，从而有效加强漏洞防范。同时，应经常关注软硬件产品和服务厂商发布的安全公告，并关注国家信息安全漏洞平台（CNVD）网站和微信公众号，对尚未推出补丁的漏洞情况，及时采取临时性技术措施进行防范。

（二）在网络关键点部署防护设备

涉事单位可根据自身的业务系统、网络特点情况，部署适合的网络安全防护设备（包括但不限于：防火墙、堡垒机、入侵检测系统、日志审计等），及时发现可能存在的计算机

安全漏洞，科学筛选、隔离非法数据，保护计算机网络的数据与信息。

（三）定期开展网络安全渗透测试和风险评估

定期开展对网络信息系统的渗透测试和漏洞扫描，及时发现网络、系统中的安全问题和风险，并进行修复加固，提升业务系统自身的安全防护水平。定期开展网络安全风险评估，从网络资产、安全漏洞、攻击威胁等方面全面评估安全风险，根据实际情况采取有效的安全措施，降低面临的安全风险。

（四）合理配置访问权限

通过有效的设置和控制网络访问权限，做到科学监控网络计算机，并定期发现、记录可能存在隐患的计算机程序，做好计算机网络端口的检查、维护、更新工作，防止网络病毒侵入网络服务器来入侵计算机系统，最大限度阻止不法份子侵入、使用、泄露、篡改计算机数据。

（五）常态化开展重要数据备份

将重要的数据资产进行本地以及异地备份，在遭受漏洞攻击后，利用备份数据快速恢复业务系统，降低损失。通过及时备份重要数据，不仅能够保护重要数据提高数据的安全性和稳定性，还能充分降低不法分子入侵计算机系统后恶意篡改、删除数据引发的风险和危机。

（六）应用数据加密技术

运用数据加密技术可保障数据安全性，同时降低漏洞攻击导致的泄露数据的可能性，提高计算机数据的安全性。

（七）检查和加强安全配置

定期修复网络安全漏洞更新漏洞补丁，关闭不必要的文件共享，关闭 3389、445 等不用的高危端口，定期更新防护系统病毒库，开启服务系统关键日志收集功能，为安全漏洞事件跟踪溯源提供基础。

针对防火墙、路由器、交换机等网络节点设备的安全访问控制策略进行优化、检查、分析，梳理出空策略、过期策略、隐藏策略、冗余策略、宽松策略、可合并策略六种可优化策略，收缩网络访问权限。通过特征检测、查杀技术提升企业被动防护能力，降低网络安全风险。

（八）加强网络安全规划

单位应制定相关的网络安全管理机制，强化网络安全管理工作的执行，提升内部人员的网络安全意识、合理、合法、安全的使用计算机网络。

定期组织网络安全培训，加强计算机应用人员、管理人员的安全风险意识和掌握计算安全漏洞防范技术与知识，并严格遵守计算机操作使用规程，安全使用网络计算机。

（九）优化漏洞及资产管理

为确保重大安全漏洞可以快速定位，涉事单位需建立资产台账，细化业务、IP、各类组件、开放端口、使用人、责

任人、上线信息等信息，可根据实际情况按需建立资产管理平台。定期在单位内部或各分支机构进行资产收集上报、同时配合技术手段定期进行资产发现及测绘工作，确保资产更新及时准确。同时还需做好资产的动态维护，针对资产上线、下线、更新等，资产台账或平台内及时变更。

（十）强化网络安全监测

梳理涉事单位现网中的安全设备，重点在安全检测与流量分析设备，日常对安全设备进行降噪，不断优化安全策略，并基于此对疑似成功的网络攻击事件，均通过网络审计设备及受影响终端进行确认，若确认攻击成果则分析攻击行为并提取特征值，在单位内部进行排查。针对有分支机构的涉事单位需组织分支机构进行全量检查并予以指导。