 DOI: https://doi.org/10.12349/iser.v4i3.1535

Analysis of Vulnerability Management Scheme

Yunxin Wang

China Telecom Corporation Limited Shaanxi Branch, Xi'an, Shaanxi, 710056, China

Abstract

With the diversification of enterprise applications and the formation of vulnerability industrialization trend, the number of vulnerabilities in the world continues to grow rapidly. In 2021, the National Information Security Vulnerability Sharing Platform (CNVD) recorded more than 18592 vulnerabilities, with an average of 50 new vulnerabilities every day. At present, network security is suffering from a serious vulnerability crisis. In the daily security operation of enterprises, the confrontation with vulnerability attacks and the management of vulnerabilities have always been a long-standing problem for administrators. According to a domestic survey of Safe Cow, nearly 20% of security personnel mentioned that they had failed to fix the loopholes in time, which caused huge losses to enterprises. The harm of vulnerabilities is getting more and more serious. In the final analysis, it is the result of the existence of system vulnerabilities and their malicious use by attackers. Devices such as vulnerability scanning can let users know clearly what vulnerabilities exist in their T system. However, most enterprises can't fix these vulnerabilities, and even those that have been proved to be extremely risky, the repair rate is less than 20%. In order to effectively deal with the exploitation of vulnerabilities, a new vulnerability management scheme is proposed, which provides reference for the subsequent

Keywords

vulnerability, vulnerability governance; scheme

浅析漏洞治理方案

王允昕

中国电信股份有限公司陕西分公司，中国 · 陕西 西安 710056

摘　要

随着企业应用多样化，漏洞产业化趋势的形成，全球漏洞数量持续快速增长，2021年国家信息安全漏洞共享平台（CNVD）收录漏洞超过18592个，平均每天新增50个，目前网络安全正在遭受严重的漏洞危机。而在企业的日常安全运营工作中，与漏洞攻击的对抗以及漏洞的管理，一直都是管理员长久以来的难题。安全牛的一项国内调查中显示，接近20%的安全人员提到，曾没有及时对漏洞进行修补，而让企业遭受巨大的损失。漏洞的危害越来越严重，归根结底，就是系统漏洞的存在并被攻击者恶意利用的结果。漏洞扫描等设备可以让用户清晰了解自身T系统存在哪些漏洞。但绝大部分企业都无法修复这些漏洞，即便是已经被证明会产生极大风险的漏洞，修复率也不足20%。为有效应对漏洞被利用情况，提出一种新型漏洞治理方案，为后续云数据中心安全服务系统建设提供参考。

关键词

漏洞；漏洞治理；方案

1 引言

据 Statista 统计，2022 年发现了 22514 个常见的 IT 安全漏洞，这是迄今报告的最高年度数字。据 SecurityWeek 信息称，2022 年出现了一些高危的零日漏洞，其中微软约占 23%，谷歌 Chrome 占 17%，苹果产品（iOS 和 macOS 零日漏洞合计）占 17%。根据 *2023 Microsoft Vulnerabilities Report* 报告显示，2022 年微软产品漏洞总数增加至 1292 个，创下该报告 10 年来的最高纪录。漏洞数量较高意味着企业面临更广泛的网络风险与攻击面，这无疑加大管理难度与资源要求。除了关注漏洞数量以外，也需关注个别漏洞带来的独特威胁与影响。某个高危漏洞的出现，也可能直接威胁企业关键系统与数据资产的安全。

漏洞可能持续不断变化，但攻击者的目标仍然不变，即让代码具有足够的权限来执行恶意任务。为实现这个目标，攻击者需要具有远程代码执行能力，能够在目标系统上启动自己的代码以及提权以确保此代码具有足够的权限运行。根据报告显示，2013 年到 2019 年，远程代码执行漏洞占比最高，2020 年到 2023 年提权漏洞占比最高。在过去三年中提权漏洞呈急剧上升趋势，2023 年更是高达总数的 55%。

调查还显示，47% 的网络安全事件是由未修补的安全漏洞导致的（如图 1 所示）。已知的安全漏洞很容易被网络罪犯利用，威胁行为者利用自动化工具同时扫描许多公司的系统中的已知漏洞。一旦发现系统漏洞，可以使用现成的利用代码进行入侵。

【作者简介】王允昕（1977–），男，中国陕西西安人，本科，从事网络安全防护、运维研究。

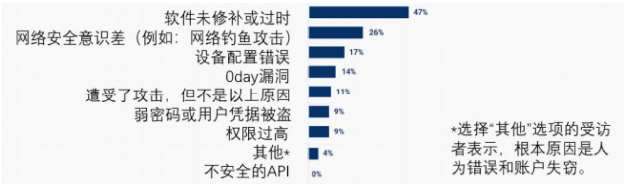

图 1 调查数据（1）

此外，调研显示有 56% 的组织以手动方式修复安全漏洞，有超过 62% 的人会选用一个终端防御系统进行防护（如图 2 所示）。

图 2 调查数据（2）

此外，根据调查显示，由于管理层支持不足、预算削减与组织结构变更等问题都可能导致安全漏洞无法得到有效处理（如图 3 所示）。当 IT 运维团队被运营问题“淹没”时，也可能导致组织的 IT 系统和基础设施中的漏洞没有得到处理。

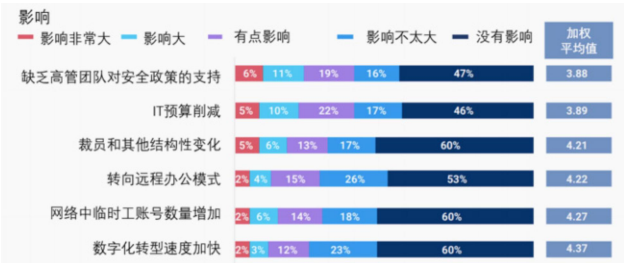

图 3 调查数据（3）

但是，即便组织得到了足够支持，想要进行有效的漏洞修复仍然困难重重。根据图 3 有 47% 的人认为系统打补丁可能引发业务中断风险，这是进行补丁修复最大的障碍之一。

调查显示 40% 的组织，需要超过一个月的时间来修复新发现的关键漏洞（如图 4 所示）。在此期间，攻击者随时都可能利用相关漏洞发起攻击，这对于组织系统而言是一个巨大的风险。

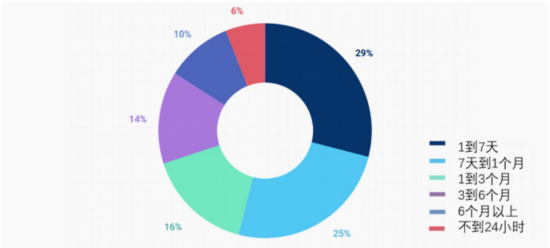

图 4 调查数据（4）

随着企业应用多样化，漏洞产业化趋势的形成，全球漏洞数量持续快速增长，2021 年国家信息安全漏洞共享平台（CNVD）收录漏洞超过 18592 个，平均每天新增 50 个，目前网络安全正在遭受严重的漏洞危机。

在企业的日常安全运营工作中，与漏洞攻击的对抗以及漏洞的管理，一直都是管理员长久以来的难题。安全牛的一项国内调查中显示，接近 20% 的安全人员提到，曾没有及时对漏洞进行修补，而让企业遭受巨大的损失。

漏洞的危害越来越严重，归根结底，就是系统漏洞的存在并被攻击者恶意利用的结果。漏洞扫描等设备可以让用户清晰了解自身 T 系统存在哪些漏洞。但绝大部分企业都无法修复这些漏洞，即便是已经被证明会产生极大风险的漏洞，修复率也不足 20%。

论文提出一种针对漏洞管理的漏洞屏蔽技术让漏洞无法被利用。通过第三方漏扫工具发现的漏洞或者结合安全服务认为需要屏蔽的漏洞，梳理出漏洞列表导入到系统中，系统会结合自身的规则自动匹配出需要屏蔽的漏洞，一旦网络中出现针对该漏洞的利用行为，可以模拟阻断报文，将该会话强制断开，从而使漏洞无效。

2 漏洞管理现状

漏洞的修复率偏低，有很多现实的原因，这些原因是客观存在的。

①漏洞的真实优先级与实际不匹配。

②不论是国外还是国内的漏洞库，都主要是对漏洞的理论危害性进行评级。例如 CVSS 评分，如果依照评分的建议修复漏洞，危急以上的漏洞将达 65% 以上，但这些危急漏洞在大多数环境下应用条件都十分苛刻，这种与真实情况不匹配的情况，导致漏洞修复浪费了大量的成本在“不必要修复”的漏洞上，而真正需要关注的漏洞却没有修复。

③系统老旧不再维护补丁。

④停止支持的应用程序和操作系统不再提供漏洞修复的补丁，如 XP。目前，据统计，超过 50% 的已知漏洞没有可修复的补丁。

⑤修复漏洞会引发风险。

⑥关键业务系统，会面临来自业务和运维团队的阻力，因为修复漏洞本身也会引发风险，可能导致业务系统短暂 / 持续的宕机。

⑦修复的人力和时间成本都很高。修复漏洞本身是一项成本很高的工作，需要投入大量人力和时间去修复漏洞，并且修复后还需验证打完补丁之后业务是否正常。

3 漏洞防护方案

面对漏洞修复空窗期的风险，关键业务漏洞修复风险，老旧系统补丁断更，监管侧的合规检查等一系列难题，依赖漏洞扫描发现漏洞，修复漏洞对应补丁的传统方式，已不能解决不断涌现的新问题。

打补丁的目的是修复漏洞，修复漏洞的目的是让这个

漏洞利用无效。我们跳出漏洞打补丁的固定思维，如果可以通过有效的手段准确、快速地屏蔽漏洞利用的动作，本质上也可以让漏洞利用无效化。漏洞治理系统通过漏洞屏蔽技术让漏洞无效化的产品。通过第三方漏扫工具发现的漏洞或者结合安全服务认为需要屏蔽的漏洞，梳理出漏洞列表导入到画方 NIDR 中，画方 NIDR 会结合自身的规则自动匹配出需要屏蔽的漏洞，一旦网络中出现针对该漏洞的利用行为，可以模拟阻断报文，将该会话强制断开，从而使漏洞无效。

4 漏洞治理平台架构

4.1 漏洞治理平台框架概述

漏洞治理平台通过漏洞扫描设备的扫描结果，或通过手动方式在系统自定义漏洞规则。系统采用 B/S 架构，包括基础管理模块、漏洞规则库模块、漏洞管理配置模块、数据采集模块。

4.1.1 基础管理模块

用于设置漏洞治理系统相关的系统功能，主要包括账号管理、通知管理、存储管理、系统安全管理等功能。

4.1.2 漏洞无效化模块

漏洞无效化模块支持对攻击者的漏洞探测和漏洞攻击等漏洞利用行为进行综合防护。

4.1.3 漏洞管理配置模块

平台核心功能，用于对防护目标资源进行针对化的漏洞防护配置，实现漏洞全生命周期的闭环管理。

主要组成包括漏洞数据导入、智能分析匹配、防护目标管理、告警拦截管理、屏被策略管理。

4.1.4 数据采集模块

漏洞治理系统的数据采集主要通过被防护资源的导入和漏洞扫描设备的扫描结果导入两种方式。

4.2 漏洞治理系统的先进性说明

4.2.1 快速部署，即插即用

旁路镜像流量部署，即插即用，不需要在每一台服务器上安装插件，也无需更改业务逻辑，对业务没有侵入性，不会利用服务器资源来解析流量。

4.2.2 多场景适用，快速阻断

不同于 agent 的方式，不局限于服务器侧漏洞，可屏蔽网络设备漏洞，同时基于算法深度优化，并采用业界最快的高性能匹配引擎，阻断足够快。图 5 为使用流程。

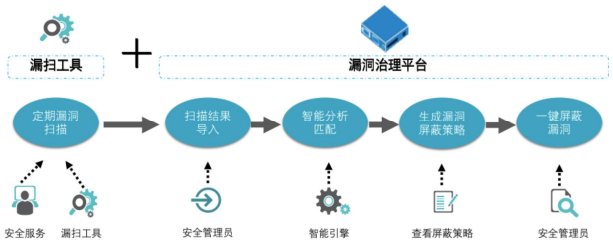

图 5 使用流程

4.2.3 漏洞治理系统的主要功能

防御恶意漏洞探测：识别分析网络中的漏洞探测行为，并开启对应的漏洞屏蔽方案，使黑客探测获取不到真实漏洞信息，帮助用户，减少被黑客利用的机会。

防御漏洞定向攻击：以“安全漏洞”为视角，针对性地匹配网络资产中的漏洞信息，精准防护网络资产中真实存在的漏洞，一旦发现资产中存在真实的漏洞攻击行为，会进行针对性的屏蔽，使漏洞探测和攻击行为失效。

防御病毒利用漏洞扩散：病毒可以通过漏洞在局域网中无限传播，通过旁路镜像的方式接入，覆盖内网流量，不但可以检测南北向流量，还可以检测东西向流量，拦截东西向的漏洞探测和攻击行为，切断利用漏洞进行病毒传播的途径。

5 方案价值

5.1 缓解安全和运维压力

可以极大地降低漏洞修补的工作量，并且能把无法修补的漏洞无效化，使之无法被利用，从而从实质上消除这些漏洞带来的风险，提升工作效率和价值。

5.2 降低合规监管风险

等保三级存在高危漏洞将无法通过等保测评，漏洞扫描是监管单位重要的检查手段，也是黑客攻击的第一步，此方案可智能识别分析网络中的漏洞利用行为，并开启对应的漏洞屏蔽方案，能够让探测漏洞的行为无探测结果，满足等保要求，降低因漏洞问题而被通报风险，减少被黑客利用机会。

5.3 实现漏洞闭环管理，降低漏洞利用机会

可根据漏洞扫描器的结果，生成漏洞屏蔽策略，计算出最佳漏洞闭环解决方案，并根据解决方案自动防护抵御漏洞探测、攻击等漏洞利用 行为，使得管理人员可以有效地跟踪资源漏洞生命周期，实现漏洞全生命周期的闭环管理，降低黑客漏洞利用机会。

6 结语

随着其他国家政府针对漏洞信息披露管控的加强，中国采用或依赖相关产品的系统将面临漏洞信息获取滞后甚至无法获取的不确定性风险，漏洞修复的空窗期被延长或无法通过原厂商及时修复，论文提出的一种漏洞治理系统可用户漏洞防护和被利用方面的质量，能够有效较少利用漏洞攻击的网络安全事件。

参考文献

[1] 汪列军.基于漏洞情报的漏洞运营实践[J].中国信息安全,2022(6).

[2] 时翌飞,冯景瑜,黄鹤翔,等.安全漏洞国际披露政策研究[J].信息安全研究,2021(3).

[3] 张静.漏洞多方协同披露机制研究[J].信息安全与通信保密,2021(8).