中数国科漏洞扫描系统

产品技术白皮书

中数国科集团

引　　言

编写目的

本文档主要阐述了中数国科漏洞扫描系统的设计背景、功能、特点、应用价值及其典型应用场景等内容，帮助您快速和全面的了解本产品。

读者对象

- 产品经理
- 销售人员
- 目标客户
- 其他想要全面了解本产品的相关人员

约　　定


注意：　　说明需要注意的信息，突出重要/关键信息、最佳实践和小窍门等。

目　　录

1 前言

1.1 漏洞的出现

漏洞主要是因为设计和实施中出现错误所致，造成信息完整性、可用性和保密性受损。漏洞通常在软件中，也存在于各个信息系统层，从协议规格到设计到物理硬件。漏洞还可能是恶意用户或自动恶意代码故意为之。重要系统或网络中单个漏洞可能会严重破坏一个机构的安全态势。

“漏洞”一词的定义是易受攻击性或“利用信息安全系统设计、程序、实施或内部控制中的弱点不经授权获得信息或进入信息系统。”这里的关键词是“弱点”。任何系统或网络中的弱点都是可防的。

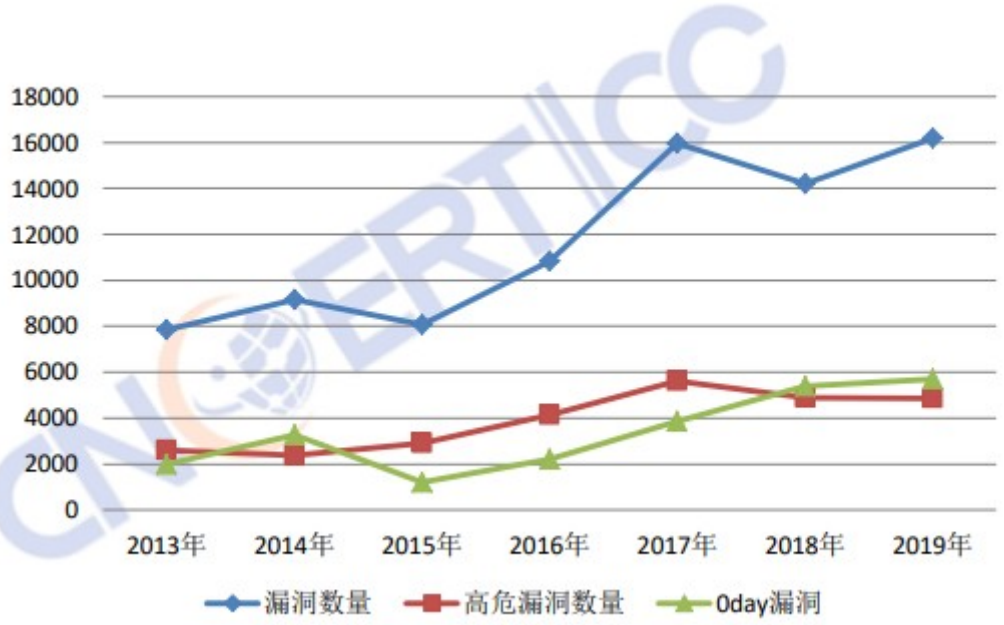
1.2 漏洞的影响

漏洞会影响到很大范围的软硬件设备，包括操作系统本身及其支撑软件，网络客户和服务器软件，网络路由器和安全防火墙等。换而言之，在这些不同

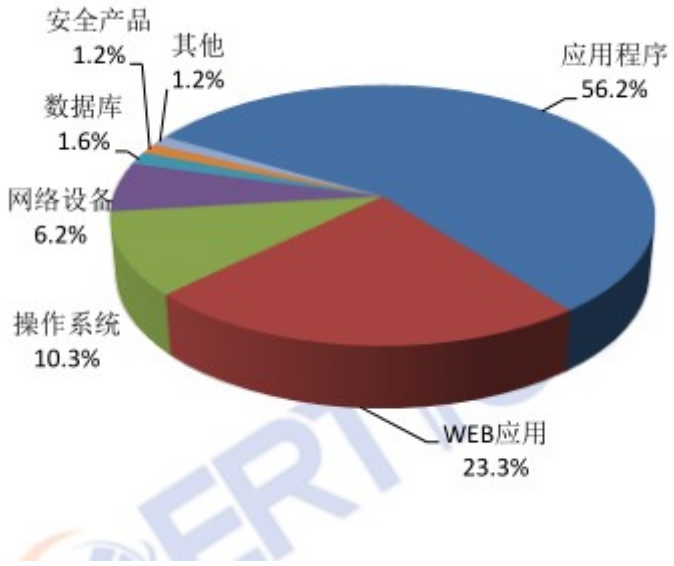
的软硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

1.3 漏洞的危害

2019 年，国家信息安全漏洞共享平台（CNVD）收录安全漏洞数量创下历史新高，收录安全漏洞数量同比增长了 14.0%，共计 16,193 个，2013 年以来每年平均增长率为 12.7%。其中，高危漏洞收录数量为 4,877 个（占 30.1%），同比减少 0.4%，但“零日”漏洞收录数量持续走高，2019 年收录的安全漏洞数量中，“零日”漏洞收录数量占比 5.2%，达 5,706 个，同比增长 6.0%。



安全漏洞主要涵盖的厂商或平台为谷歌（Google）、WordPress、甲骨文（Oracle）等。按影响对象分类统计，排名前三的是应用程序漏洞（占56.2%）、Web 应用漏洞（占23.3%）、操作系统漏洞（占10.3%）。CNVD全年通报涉及政府机构、重要信息系统等关键信息基础设施安全漏洞事件约2.9万起，同比大幅增长42.1%。



而且，信息系统配置操作是否安全也是安全风险的重要方面，安全配置错误一般是由人员操作失误导致。虽然现在有了配置检查 Checklist、行业规范和等级保护纲领性规范要求让运维人员有了检查安全配置的依据，但是面对网络中种类繁杂、数量众多的设备和软件，如何快速、有效的检查安全配置，识别与安全规范不符合的项目，以达到整改合规的要求，这也是运维人员要面临的

难题。

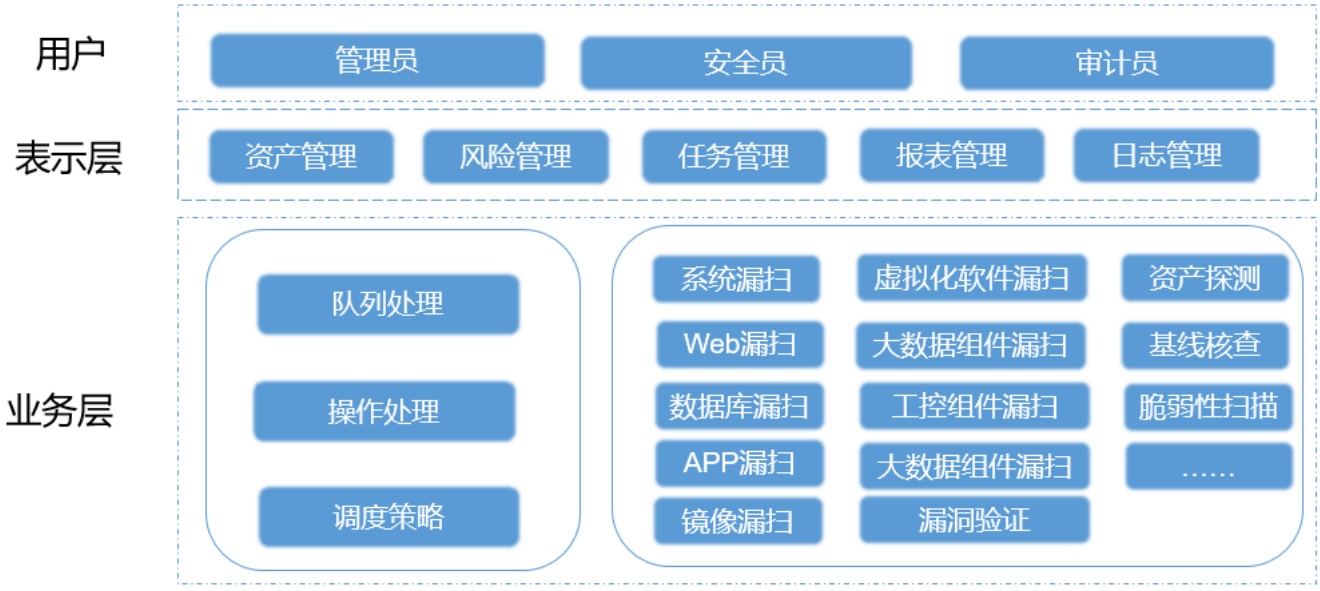
根据美国软件工程研究所估算，如果系统能够及时安装合适的软件补丁，可以避免95%以上的网络入侵。而且，很多安全漏洞、错误配置是可以通过网络漏洞管理系统进行检测与发现的，并通过漏洞修复和加固，防患于未然。因此，一个自动化、全局性的网络漏洞管理系统对用户就显得十分必要。

同时，随着国家信息安全风险评估和等级保护工作的逐步深入，如何减少法规遵从和安全风险的压力，成了信息化建设的当务之急。

2 产品概述

中数国科漏洞扫描系统包含了空间资产管理、系统漏洞扫描、WEB 漏洞扫描、基线配置核查、移动应用扫描、镜像漏洞扫描、模板管理、报表管理、辅助工具、日志管理、系统管理等模块，能够全面、精准地检测信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等，在信息系统受到危害之前为管理员提供专业、有效的漏洞分析和修补建议。并结合可信的漏洞管理流程对漏洞进行预警、扫描、修复、审计，防患于未然。

产品适用于政府、军队、公安、教育、电力、医疗、金融、运营商等行业，帮助用户解决目前所面临的各类常见及最新的安全风险，同时满足如等级保护行业规范等政策法规的安全建设要求。



3 主要功能

3.1 系统扫描模块

中数国科漏洞扫描系统能够全方位、多侧面对主流的操作系统、应用服务、数据库、网络设备、虚拟化平台、大数据组件、、工业控制系统等进行实时、定期的系统漏洞扫描和分析。支持的 Windows 包括：NT、2000、XP、2003、Win7、Win10、2008、2012、2016 等。支持的 Linux 包括：Amazon Linux、CentOS、Debian、Fedora、Red Hat、SuSE、Ubuntu 等。支持的 Unix 包括：AIX、FreeBSD、HP-UX、Solaris、Mac OS X 等。支持的 WEB 应用服务包括 IIS、Apache、Tomcat、Websphere、Weblogic、Nginx 等。支持的应用软件包括：Microsoft Internet Explorer、Office、RealPlayer、Outlook、Adobe Flash 等。支持的数据库包括：Oracle、Mysql、DB2、Informix、MSSQL、Sybase 等。支持的网络设备包括：思科 Cisco、华为 HUAWEI、华三 H3C 等。支持的安全设备包括：juniper 等。支持的虚拟化平台包括：Vmware EXSi、

Citrix XenServer、Microsoft Hyper-V 等。支持的云平台包括：VCenter、OpenStack、Eucalyptus 等。支持的大数据包括：Hadoop、Spark、HBase、Hive 等。支持的工业控制系统包括：工控协议识别支持对 S7、Proconos、PCWorx、Omron、Modbus、MMS、MelSecq、IEC104、Fox、ENIP、dnp3、Crimson、MelSecq、Bacnet、Profibus、PROFINE 等工控协议。

系统支持智能服务识别、安全优化扫描、授权登录扫描、恶意代码检测等，具备的系统漏洞知识库的检测脚本大于 260000 条，提供了详细的漏洞描述和漏洞修复建议，方便用户及时发现信息系统中存在的安全漏洞，通过安全加固防患于未然。

3.2 WEB 扫描模块

中数国科漏洞扫描系统具备强大的 Web 应用漏洞安全检测能力，全面支持 OWASP TOP 10 漏洞检测，比如 SQL 注入、跨站脚本攻击 XSS、网站挂马、网页木马、CGI 漏洞等。支持的协议包括：HTTP、HTTPS 等。支持的 WEB 服务器包括：IIS、Websphere、Weblogic、Apache、Tomcat、Nginx 等。支

持登录预录制功能，能够根据用户操作，录制并指定 Web 扫描 url，使产品能够扫描和分析一些常规页面爬取程序检测不到的 url。方便用户及时发现 WEB 网站中存在的安全漏洞，避免信息安全事件的发生。

3.3 基线配置核查模块

中数国科漏洞扫描系统具备先进的安全基线配置核查能力，可以对目标系统进行自动化的基线检测、分析，并提供专业的配置加固建议与合规性报表。支持的操作系统包括：Windows、Linux（Centos、Debian、Fedora、Redhat、Suse、Ubuntu 等）、Unix（Aix、HP-UX、Solaris 等）、国产操作系统（中标麒麟、欧拉、红旗等）等。支持的中间件包括：IIS、Apache、Tomcat、Weblogic、Websphere、Nginx、Jboss、Resin 等。支持的数据库包括：Oracle、Mysql、DB2、Informix、Mssql、Sybase 等。支持的网络设备包括：思科、华三、华为等。支持的安全设备包括：juniper、天融信、华为、网神等。支持的虚拟化平台包括：Vmware EXSi、XenServer 等。支持的大数据包括：Hbase、Hive、Spark、Storm、Kafka 等。

系统支持多种协议远程登录目标系统进行基线核查，包括 SMB、Telnet、SSH 等。支持 Agent 本地检测，提供了专用的 windows 配置检查工具。支持在线设备基线核查和离线设备基线核查。基线核查过程只检查系统的配置情况，不对系统配置进行任何修改，确保业务持续性和业务安全。让安全配置维护工作变得有条不紊而且简单、易于操作，方便用户及时发现信息系统中存在的不安全配置，提高目标系统的安全防护水平。

3.4 镜像扫描模块

中数国科漏洞扫描系统可以检测出 Docker 镜像漏洞、高危风险以及不安全的配置。Docker 漏洞知识库数量大于 120000 条，包括了权限许可、目录遍历、安全绕过、拒绝服务、代码注入等漏洞。从而能够全面发现 Docker 中存在的各种安全风险，及时通过安全加固，提高 Docker 安全水平。

3.5 移动扫描模块

中数国科漏洞扫描系统支持对 Android、ios 上的移动应用（APP）进行漏

洞扫描，采用静态分析的方式，准确发现 APK 中存在的组件安全、配置安全、数据安全和恶意行为等安全风险。从而大幅提升移动 APP 的安全性，避免因 APP 漏洞造成业务损失。

3.6 资产发现与管理模块

中数国科漏洞扫描系统综合运用多种手段，全面、快速、准确的主动发现被扫描网络中的存活主机，准确识别其属性，包括主机名称、IP 地址、端口、操作系统、软件版本、负责人、地区等，为进一步漏洞扫描做好准备，支持发现网段中存活 IP、端口、服务，同时资产列表可以展示操作系统、端口数、严重漏洞数、高危漏洞数、中危漏洞数等信息。

4 产品特色

4.1 精准的扫描技术

中数国科漏洞扫描系统采用自主研发的底层核心引擎，拥有先进的扫描技术，不断提高执行效率和调度效率。

其中，系统漏洞扫描支持智能服务识别、授权登录扫描、安全优化扫描、恶意代码检测等。WEB 漏洞扫描支持 Cookie 认证、会话录制、漏洞验证等。基线配置核查支持 SMB、Telnet、SSH 等多种协议的远程检测，多种操作系统和网络设备的离线检测，提供了专用的 windows 配置检查工具。工控漏洞扫描支持无损的工控漏洞扫描技术，支持远程指纹探测技术，也支持离线比对工控漏洞知识库。镜像漏洞扫描支持检测 Docker 漏洞、Docker 镜像漏洞、木马后门，以及不安全的配置。支持大数据漏洞扫描对主流大数据组件进行漏洞扫描和安全配置合规性检查。

4.2 丰富的漏洞知识库

中数国科漏洞扫描系统的漏洞知识库涵盖了各种主流操作系统、应用服务、数据库、网络设备、虚拟化平台、大数据、视频监控系统、工业控制系统等。漏洞知识库数量国内领先，每周至少升级一次。漏洞相关信息支持全中文，兼容 CVE 等标准，漏洞修复建议清晰、详细，可操作性强。

其中，系统漏洞知识库的检测脚本大于 240000 条，提供了详细的漏洞描述和对应的修补措施和安全建议。WEB 漏洞知识库的检查策略大于 10000 条，涵盖了 SQL 注入、跨站脚本攻击 XSS、网站挂马、网页木马、CGI 漏洞等。数据库漏洞知识库的扫描策略大于 3000 条，覆盖了权限绕过漏洞、SQL 注入漏洞、访问控制漏洞等。工控专有的漏洞知识库数量大于 4000 条，从而全面发现信息系统中存在的各类安全风险。

4.3 直观的报表管理

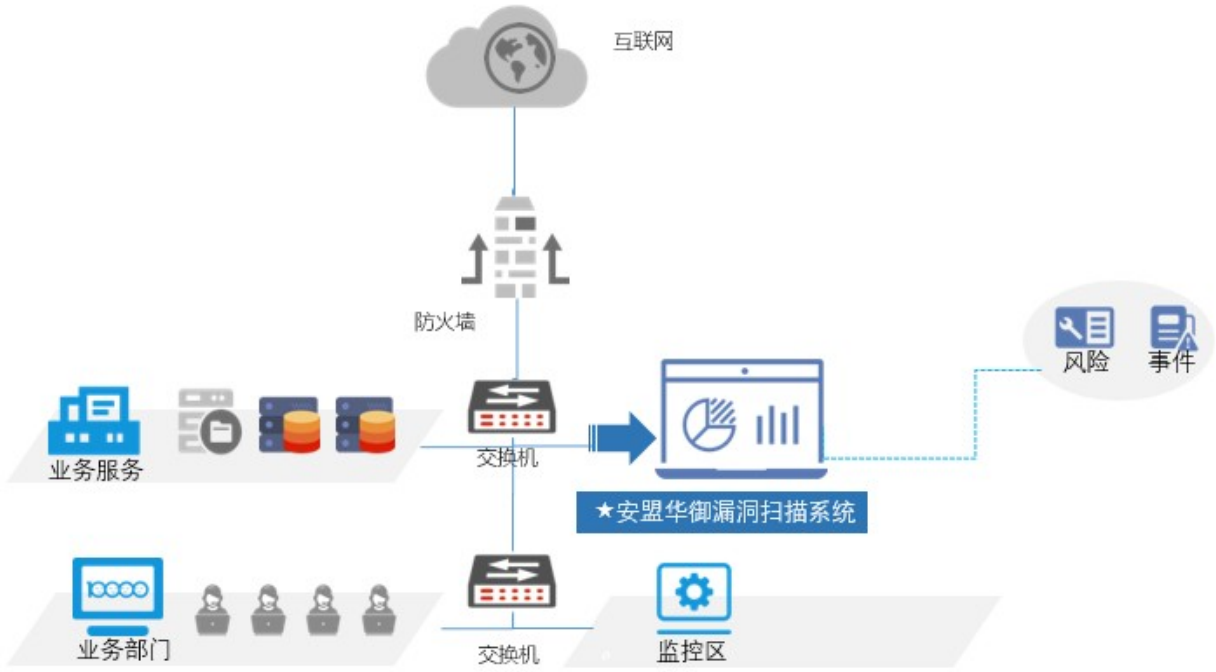
中数国科漏洞扫描系统扫描结果通过自定义的方式灵活的呈现给用户，支持各类报表格式输出，并提供漏洞分级、相应加固建议方案以及自定义报表内

容。提供定性的趋势分析、定量的风险分析，更加直观地了解当前网络安全状况。

5 产品部署

中数国科漏洞扫描系统是根据网络 IP 地址分布情况进行配置的，它可以部署在网络的任何地方，只要能够访问到要进行安全评估的目标系统就能够正常工作。

中数国科漏洞扫描系统的部署图如下图所示：



6 应用案例

企业信息系统投运前测试

- **场景特点**：在企业内部信息系统投入使用前，将漏洞扫描系统接入到网络中，开展投运前安全漏洞扫描。

- **用户收益**：使用中数国科漏洞扫描系统实现系统脆弱性评估，根据扫描报告漏洞分级、加固建议方案内容，有针对性地修复信息系统中存在的风险漏洞，避免投产后造成更大的网络安全隐患。

网络安全测评/风险评估

- **场景特点**：针对企业单位整体系统网络进行安全测评或风险评估时，使用漏洞扫描系统实现系统脆弱性评估。

  用户收益：对整个系统网络形成评估报告，提供网络资产漏洞详细信息展示及安全修补方案建议，形成风险趋势分析报表，帮助评估人员掌握系统安全脆弱性，同时满足合规检查资质要求。