



天镜脆弱性扫描与管理系统 V6.0

天镜脆弱性扫描与管理系统（以下简称“天镜”）是启明星辰自主研发的基于网络的脆弱性分析、评估与管理系统。

天镜遵循启明星辰在总结多年市场经验和客户需求基础上提出的“发现—扫描—定性—修复—审核”的安全体系构建法则，综合运用多种国际最新的漏洞扫描与检测技术，能够快速发现网络资产，准确识别资产属性、全面扫描安全漏洞，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而帮助用户在弱点全面评估的基础上实现安全自主掌控。

天镜通过综合运用多种手段（主机存活探测，智能端口检测，操作系统指纹识别等）全面、快速、准确的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、设备类型、端口情况、操作系统以及开放的服务等，为进一步脆弱性扫描做好准备。

同时，天镜的资产管理功能能够为用户的 IT 资产提供方便，同时作为脆弱性风险评估的基础部分，为评估主机和网络的脆弱性风险提供依据。

渐进式的扫描方法能够让天镜利用已经发现的资产信息进行针对性扫描，发现主机上不同应用对象（操作系统和应用软件）的弱点和漏洞，同时保证扫描过程的快速和结果的准确。目前，天镜可检测的漏洞数量已经超过 250000 条，扫描对象涵盖各种常见的网络主机、操作系统、数据库系统、网络设备、应用系统、常用软件、云计算平台、Apple 平台等。





一、主要功能

功能项	功能描述
漏洞扫描能力	内置漏洞知识库 25 万，web 漏洞数量 3200 种，数据库 2800 种，CVE 漏洞数 80000。
	支持对主流操作系统、web 服务器、网络主机、移动设备、应用及软件等资产提供脆弱性评估服务。
	支持对主流虚拟化软件平台进行扫描，包括：OpenStack、KVM、Vmware、Xen、Docker、Huawei FusionSphere 等，支持漏洞库定期更新。
	支持对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、SQL SERVER、GaussDB、DB2、MySQL、达梦、人大金仓、优炫、PostgreSQL、Redis 等，能够扫描的数据库漏洞扫描方法≥2600 种。
	支持漏洞查询、策略复制以及根据市场情况及时更新应急响应策略。
	支持 40 种以上默认扫描策略模板，如常规安全扫描，中高危漏洞扫描，高危漏洞扫描，web 服务组件扫描，网络设备扫描，云平台漏洞扫描，虚拟化扫描，主机信息收集，攻击性扫描，SQL SERVER 数据库扫描，Apple 类扫描，视频监控类扫描等等，同时支持漏洞的查询，策略的复制，针对市场应急响应的漏洞提供应急响应策略模板。
	支持弱口令检测，支持对国产操作系统的检测，支持包含 DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、的弱口令探测。
	支持灵活的扫描策略自定义功能，提供策略编辑向导和详细漏洞信息，支持以系统类型、漏洞类型、危险级别、CVE 等不同视图显示漏洞，支持策略的导入、导出、修改以及合并。
	支持首页全面展示风险分布及趋势图表，包括主机风险分布、站点风险分布、漏洞风险分布、漏洞 top10、资产风险值趋势、资产风险分布趋势；
	支持资产管理功能，资产信息包含资产名称、IP、MAC、负责人等，并可按需添加自定义属性；
	支持以 txt、csv、dat、xls 等格式进行资产列表的导入。
	支持每个资产历史扫描的风险趋势图显示，缺省显示最后 24 次扫描结果的趋势显示。
	支持部门和资产的分级管理，支持通过资产编号、资产名称和资产 IP 进行资产查询功能。
	报告包含漏洞详述和修补方案，对于常见补丁类漏洞能够提供相关的补丁下载链接。
	报告中的漏洞具备统一的 CVSS 国际标准评分，以准确衡量漏洞的危险级别，为漏洞修补工作的优先级提供指导。





	支持扫描任务完成后自动生成指定格式和内容的报表, 格式包含 pdf、word、excel 等;
	支持导出 XML、html、word、excel、PDF 等多种常见格式。
	具备报表功能, 报表支持综述报表及主机报表, 可自定义安全结论。
接口规范	支持将日志数据接入安全管理系统。

二、产品规格

产品型号	TJCS-UVS2200-JZ03
产品名录情况	产品为《安防设备产品》名录中选取符合该项目性能要求的产品;
产品规格	2U 机架式设备, 配置千兆电口 6 个, 千兆光口 4 个, 万兆光口 2 个, 接口扩展槽位 1 个, 冗余电源; 产品在《安防设备产品》名录中, 符合该项目性能要求的产品。
性能说明	支持 200 个 Web 域名扫描授权, 并发扫描 30 个 web 扫描任务; 提供无限制 IP 扫描授权, 并发扫描无限制个系统扫描任务, 并发扫描 100 个 IP 地址;
电源 (AC)	100-240V AC
频率	50-60Hz
输入电流	5-3A
功率	350W
储存温度	0-40℃
气压	-40-70℃
工作湿度	86-106KPa
储存湿度	5%-90%, 无凝结
串口	1 (RJ45 串口)
USB	2 个

