ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1142—2014

信息安全技术
主机安全检查产品安全技术要求

Information security technology—
Security technical requirements for host security inspecting products

2014-03-14 发布　　2014-03-14 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部网络安全保卫局、蓝盾信息安全技术股份有限公司、公安部第三研究所。

本标准主要起草人：赵云、顾健、张俊兵、张奕、邱梓华、沈亮、张笑笑、宋好好、陆臻、俞优、陈彬。

引　言

本标准详细描述了与主机安全检查产品安全环境相关的假设、威胁和组织安全策略，定义了主机安全检查产品及其支撑环境的安全目的，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本标准基本级参照了 GB/T 18336.3—2008 中规定的 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了主机安全检查检查应满足的安全技术要求，但对主机安全检查产品的具体技术实现方式、方法等不做要求。

信息安全技术
主机安全检查产品安全技术要求

1 范围

本标准规定了主机安全检查产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于对主机安全检查产品的设计、开发及检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336—2008(所有部分) 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 18336—2008(所有部分)和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

代理 agent

安装在被检查的主机上，用于收集主机各项配置信息的组件。

3.2

管理控制台 management console

用于对收集到的配置信息进行集中存储和分析，并进行引擎管理、安全检查策略配置、报警管理、事件响应以及其他管理工作的组件。一个控制台可以管理多个引擎。

3.3

检查 inspect

通过引擎对主机的安全配置进行收集和分析，并在控制台集中显示的过程。

4 主机安全检查产品描述

产品由代理和管理控制台组成，根据预先定义的安全策略模版，通过管理控制台对安装了代理的主机进行安全性检查，代理收集数据，管理控制台分析数据并生成报告。达到发现其安全配置方面存在的问题的目的，此外主机安全检查产品本身及其内部的重要数据也是受保护的资产。

检查的项目常见的包括几个方面：配置检查，系统资源(CPU、内存、硬盘)，杀毒软件、进程、服务，系统共享资源，启动项，外围接口设备，系统账户，软件安装，硬件配置，网络连接，系统漏洞。

主机安全检查产品以 C/S 方式部署或者单机方式部署，并执行安全功能。其安全检查的目标是安装了引擎的主机。