

ICS 35.240

A 90

GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL_JGF_04-011 0101—2006

信息安全技术 远程主机监测产品检验规范

2006-01-01 发布

2006-02-01 实施

公安部计算机信息系统安全产品质量监督检验中心 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 产品安全功能要求	1
4.1 远程主机监测功能	1
4.2 安全功能	2
4.3 审计功能	2
5 产品安全保证要求	2

前 言

为了规范全国远程主机监测产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对远程主机监测产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局批准。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

信息安全技术 远程主机监测产品检验规范

1 范围

本规范规定了远程主机监测产品的安全功能要求和安全保证要求。
本规范适用于远程主机监测产品的开发及检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idt ISO/IEC 15408-3:1999）

3 术语和定义

3.1 远程主机监测

采用引擎(agent)/控制台(console)结构，在远程主机上安装引擎,通过控制台对远程主机上的活动进行监测的产品。

4 产品安全功能要求

4.1 远程主机监测功能

远程主机监测产品必须具备下述 4.1.1、4.1.11、4.1.12 的功能，同时应在下述 4.1.2 到 4.1.10 的监测功能中至少包括 2 项。

4.1.1 在线状态监测

应提供对远程主机在线状态、引擎运行状态监测的功能。

4.1.2 系统资源情况监测

提供对远程主机 CPU、内存、硬盘、文件等系统资源的使用情况进行监测的功能，检测范围至少包括 2 项。

4.1.3 软件安装情况监测

提供对远程主机上软件安装的情况进行监测的功能。

4.1.4 所开服务情况监测

提供对远程主机上所开服务的情况进行监测的功能。

4.1.5 外围接口设备使用监测

提供对远程主机串口、并口、USB 口、软驱、光驱等外围接口设备的使用监测的功能，监测范围至少包括 2 项。

4.1.6 进程监测

提供对远程主机的进程进行监测的功能。

4.1.7 上网情况监测

提供对远程主机的上网活动如：HTTP、POP3、SMTP、FTP、TELNET 等进行监测的功能，并能对监测结果进行记录。

4.1.8 非授权外联监测

提供对远程主机在策略允许之外通过 modem、无线设备等非授权途径与外部网络进行连接的活动进行监测的功能。

4.1.9 屏幕截取

提供对远程主机进行屏幕截取的功能。

4.1.10 键盘记录

提供对远程主机的键盘活动进行监测的功能，并能对监测结果进行记录。

4.1.11 集中管理

应提供对多台远程主机进行集中统一管理的能力，能提供主机监测策略的集中定制，并可以分发应用到相应主机上。

4.1.12 远程保密传输

应对从引擎到控制台传输的所有信息采取保密措施。

4.2 安全功能

4.2.1 引擎的自身保护功能

- a) 应采取防止非授权用户强行终止引擎程序运行的措施；
- b) 应采取防止非授权用户强制取消引擎程序在系统启动时自动加载的措施；
- c) 应采取防止非授权用户强行卸载、删除或修改引擎程序的措施。

4.2.2 管理员身份鉴别

应保证只有授权管理员和可信主机才有权使用产品的管理功能，对授权管理员和可信主机应进行身份鉴别。

4.2.3 管理员权限

- a) 管理员属性修改（更改密码等）；
- b) 启动、关闭全部或部分监测功能；
- c) 修改远程主机监测产品其它安全策略。

4.3 审计功能

4.3.1 审计数据生成

应至少能对下列事件生成日志：

- a) 远程主机监测产品的启动和关闭；
- b) 管理员鉴别成功和失败；
- c) 其它重要操作，如增加、删除管理员，存档、删除、清空日志等。

应在每一个日志记录中记录事件发生的日期和时间、事件描述。

4.3.2 审计管理

应提供下列日志管理功能：

- a) 只允许授权管理员访问日志记录；
- b) 提供对日志记录的查询功能；
- c) 授权管理员能存档、删除和清空日志记录。

5 产品安全保证要求

安全保证要求按 GB/T 18336.3—2001 第二级执行。
