ICS 35.040
L 80

GA

# 中华人民共和国公共安全行业标准

GA/T 1536—2018

# 信息安全技术
# 计算机主机安全检测产品测评准则

Information security technology Testing and evaluation criteria for detection products of host computer security

2018－12－26 发布　　2018－12－26 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：国家计算机病毒应急处理中心、天津市公安局网络安全保卫总队、江苏通付盾信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、北京天融信科技有限公司、南开大学、北京安天网络安全技术有限公司。

本标准主要起草人：陈建民、刘彦、杜振华、黄一斌、曹鹏、杨键、赵晓明、张韫菁、张瑞、张鑫、王文一、肖新光、赵焕菊、张振伟、崔婷婷、徐雨晴、王龑、贾春福、舒心、李菊、孙波、李冬。

# 信息安全技术 计算机主机安全检测产品测评准则

## 1 范围

本标准规定了计算机主机安全检测产品的受检要求、测试指标要求、功能要求、测试方法、报告格式及评级方法。

本标准适用于计算机主机安全检测产品的开发和检测。

## 2 规范化引用文件

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/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GA 243-2000 计算机病毒防治产品评级准则

GA/T 757-2008 程序功能检验方法

## 3 术语和定义

GB/T 18336.3-2015、GA 243-2000、GA/T 757-2008界定的以及下列术语和定义适用于本文件。

3.1

**操作系统安全** operating system security

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.2

**用户标识** user identification

用来标明用户的身份，确保用户在系统中的唯一性和可辨认性，一般用名称和用户标识符（UID）来标明系统中的一个用户。

3.3

**用户鉴别** user authentication

用特定信息对用户身份的真实性进行确认。

3.4

**安全策略** security policy

对计算机信息系统中与安全相关的资源，尤其是敏感信息进行管理、保护、控制和发布的规定和实施细则。

3.5

**访问控制** access control

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。

3.6

**数据完整性** data integrity

数据没有遭受以未授权方式所做的篡改或破坏。

3.7

**安全审计** security audit

为了测试系统的控制是否足够，为了保证与已建立的策略和操作堆积相符合，为了发现安全中的漏洞，以及为了建议在控制、策略和堆积中做任何指定的改变，而对操作系统记录与活动的独立观察和考核。

## 4 受检要求

### 4.1 检验周期

检验机构对程序版本发生重大升级或名称发生改变的计算机主机安全检测产品应进行检验；同时，可以根据安全威胁和国家标准与法规的发展情况对计算机主机安全检测产品进行专项检验。

### 4.2 测试用例要求

受检企业应提交其产品检验用的测试用例。

### 4.3 资料要求

本项要求包括：

a) 受检企业应提交产品研发人员的个人简历；
b) 受检企业应提交产品的中文使用说明书；
c) 受检企业应提交核封完整的正式产品。

## 5 测试指标要求

### 5.1 产品载体

主机安全检测产品单机版应提供以下载体的产品检测介质，并具有在以下介质的直接执行能力：

a) 光盘；
b) U 盘。

主机安全检测产品网络版除需提供单机版的检测介质外，还需要提供用于检测程序下发和结果汇总的便携式的主机安全检测工作站设备。

### 5.2 检测病毒能力

本项要求包括：

a) 对病毒样本基本库至少能检测其中的 95%；
b) 对流行病毒样本库至少能检测其中的 98%；
c) 对特殊格式病毒样本库至少能检测其中的 95%。

## 6 功能要求

### 6.1 身份鉴别

#### 6.1.1 口令鉴别

计算机主机安全检测产品应能够对操作系统口令信息复杂度进行识别，并通过分析提取信息判断用户口令是否合规。对不合规的弱口令与空口令应进行提示，并形成检查报表。

#### 6.1.2 用户鉴别

计算机主机安全检测产品应能够对操作系统用户信息进行识别，通过分析提取信息判断用户和组以及定义它们的属性构成。并判断用户标识是否具有唯一性，对非唯一性用户名进行提示并进行锁定，并形成检查报表。

### 6.2 访问控制

#### 6.2.1 文件权限

计算机主机安全检测产品应能够提取操作系统重要目录或文件访问权限，判断是否存在文件权限风险，并对操作系统内用户角色及权限分配进行提取，形成检查报表。

#### 6.2.2 默认共享

计算机主机安全检测产品应能够对操作系统内网络共享进行检测，判断是否存在共享风险，并形成检查报表。

### 6.3 安全审计

#### 6.3.1 审计策略

计算机主机安全检测产品应能够对提取操作系统审计策略，并能够根据审计策略配置判断是否存在配置风险，并形成检查报表。

#### 6.3.2 日志

计算机主机安全检测产品应能够对操作系统内日志服务或审计服务进行检测，判断日志服务或审计服务运行状态，并形成检查报表。

### 6.4 剩余信息保护

计算机主机安全检测产品应能对操作系统用户鉴别信息所在的存储空间，是否在被释放或在分配给其他用户前得到完全清除进行检测。

### 6.5 入侵防范

#### 6.5.1 系统补丁

计算机主机安全检测产品应能够提取操作系统已安装的补丁列表，能够根据系统补丁安装状况，列出尚未修补的高危病毒，生成提示报表，并具备补丁分发功能。

#### 6.5.2 网络状况

计算机主机安全检测产品应能够提取并记录操作系统当前网络的配置情况，含网络地址、子网掩码、网关IP地址、域名系统、端口活动情况、进程、进程与端口的绑定情况，并形成检查报表。

### 6.6 恶意代码防范

计算机主机安全检测产品应能够检测操作系统是否安装有反恶意代码软件，检测反恶意代码软件病毒库是否定期自动更新。并能够提供自带恶意代码检测软件，对操作系统进行恶意代码检测。

### 6.7 资源控制

计算机主机安全检测产品应能对操作系统的终端接入方式、网络地址范围生成报告，并能够检测根据安全策略设置登录终端的操作超时锁定。

### 6.8 数据库检测

计算机主机安全检测产品应能对主机中的数据库用户身份标识进行提取，包括主流数据库：MySQL、SQL Server、Oracle等，并检测数据库账户口令是否存在弱口令与空口令。

## 7 测试方法

测试方法按GA/T 757-2008的规定。

## 8 报告格式

产品检验结果及评分表格式见表1。

**表1 产品检验结果及评分表**

| 序号 | 检验项目 | 分数 | 备注 |
|---|---|---|---|
| 1 | 基本病毒检测 | 15 | |
| 2 | 流行病毒检测 | 15 | |
| 3 | 特殊格式病毒检测 | 5 | |
| 4 | 身份鉴别 | 10 | |
| 5 | 访问控制 | 10 | |
| 6 | 安全审计 | 10 | |
| 7 | 剩余信息保护 | 10 | |
| 8 | 入侵防范 | 10 | |
| 9 | 恶意代码防范 | 5 | |
| 10 | 资源控制 | 5 | |
| 11 | 数据库检测 | 5 | |

## 9 评级方法

本项要求包括：

a) 按表 1 规定的检验项目对受检产品进行评分；

b) 受检产品未满足检验项目要求,则该项分值为零, 满足检验项目要求,则该项分值按表 1 计算；

c) 按受检产品所得总分数确定产品的级别，级别划分见表 2。

**表2 产品检验结果及评分表级别划分**

| 序号 | 分值 | 级别 |
|---|---|---|
| 1 | 71-80分 | 一级 |
| 2 | 81-90分 | 二级 |
| 3 | 90分以上 | 三级 |