

ICS 35.240
CCS A 90

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 1142-2014

**Information security technology. Security technical
requirements for host security inspecting products**

信息安全技术 主机安全检查产品安全技术要求

(English Translation)

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: Ministry of Public Security

Table of Contents

Introduction

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Product Description 1 Host Security checks

5 2 Security Environment

5.1 Hypothesis

5.2 Threat

5.3 3 Organization for Security Policy

6 Security objectives

6.1 Product Safety Objective

6.2 Environmental security objectives

7 Security functional requirements

7.1 Policy formulation

7.2 Check function

7.3 Baseline function

7.4 Response Function

7.5 Analysis of test results

7.6 Stability and fault tolerance

7.7 Centralized management

7.8 Identification and authentication

7.9 Security Management

7.10 Audit

7.11 7 upgrades

8 8 Security assurance requirements

8.1 Configuration Management

8.2 Delivery and Operation

8.3 Development

8.4 Guidance document

11 8.5 Life Cycle Support

8.6 Test

- 8.7 Vulnerability assessment
- 9 Basic principles of technical requirements
 - 9.1 Security functional requirements Fundamentals
 - 9.2 Security assurance requirements 14 Fundamentals
- 10 Classification of claim
 - 10.1 Overview
 - 10.2 Classification of security functional requirements
 - 10.3 Classification of security assurance requirements

Foreword

This standard was drafted in accordance with GB/T 1.1-2009 given rules.

This standard was proposed by the Ministry of Public Security Network Security Protection Agency.

This standard is under the jurisdiction of the Ministry of Public Security Information System Standardization Technical Committee.

This standard was drafted. Ministry of Public Security of Computer Information System Security Product Quality Supervision and Inspection Center, Ministry of Public Security Network Security Protection Agency, blue Shield Security Technology Co., Ltd., Third Institute of Ministry of Public Security.

Introduction

This standard is described in detail and host security checking product safety environment-related assumptions, threats and organizational security policies defined host security Full security purposes check the product and its supporting environment, demonstrated by the basic principles of security functional requirements and be able to trace the products covered by safety purposes, Security purposes can be traced back cover and secure environment-related assumptions, threats and organizational security policies.

The standard base-level reference to GB/T 18336.3-2008 prescribed level EAL2 security assurance requirements, and enhance the level at EAL4 level Security assurance requirements based on the vulnerability analysis requires upgrade to an attacker can withstand moderate attack potential attack.

This standard only gives the host security checks security checks should meet the technical requirements, but the host security inspection product specific technical implementation Now way, way, etc. is not required.

Information Security Technology Host Security check product safety technical requirements

1 Scope

This standard specifies the security features host security inspection product requirements, security assurance requirements and grading requirements.

This standard applies to the host security checks product design, development and testing.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB 17859-1999 computer information system security protection classification criterion
GB/T 18336-2008 (all parts), Information technology - Security techniques - Information Technology Security Evaluation Guidelines GB/T 25069-2010 Information security technology terms

3 Terms and Definitions

GB 17859-1999, GB/T 18336-2008 (all parts) and GB/T 25069-2010 defined and the following terms and definitions Meaning applicable to this document.

Agent agent

Installed on the host to be checked, the configuration component for collecting host information.

Management Console for configuration information collected for centralized storage and analysis, and engine management, security policy configuration checks, alarm management, things Parts and components in response to other management. A console can manage multiple engines.

Check inspect

Security configuration hosts collected and analyzed by the engine, and focus on the process of the console display.

4 Host security checks Product Description

Product composition by the agent and management console, security policies based on predefined templates, through the management console to install the agent home Machine security checks, the agent collects data, the management console analyze data and generate reports. Achieve its security configuration found in the purpose of the issue, in addition to a host of important data security check of the product itself and its interior is protected by assets.

Check the project includes several common areas. configuration checks, system resources (CPU, memory, disk), anti-virus software, processes, services, System shared resources, startup items, peripheral interface devices, system accounts, software installation, hardware configuration, network connection, system vulnerabilities.

Host Security checks products to C/S standalone deployment or deployment, and perform security functions. Its goal is security check Installed engine host.