

ICS 35.240
CCS A 90

GA

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

GA/T 1392-2017

**Information security technology - Security technical
requirements for hosts file monitoring products**

信息安全技术 主机文件监测产品安全技术要求

(English Translation)

Issued on: April 19, 2017

Implemented on: April 19, 2017

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Host file monitoring Product Description
5 General Description
5.1 Safety Technical Requirements Classification
5.2 Security classification
6 Safety function requirements
6.1 Security Policy Customization
6.2 Document Monitoring
6.3 Report
6.4 Operating System Support
6.5 Alarm function
6.6 Automatic recovery
6.7 Conduct Audit
6.8 Safety Management
6.9 Self protection
6.10 Audit Log
6.11 Remote Management Encryption
6.12 Centralized group management
6.13 System alarm
7 Security Requirements
7.1 Development
7.2 Guidance Document
7.3 Life Cycle Support
7.4 Test
7.5 Vulnerability Assessment
8 Grade division requirements
8.1 Overview
8.2 Classification of safety function requirements
8.3 Security Assurance Requirements Classification

Foreword

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

This standard proposed by the Ministry of Public Security Network Security Bureau.

This standard by the Ministry of Public Security Information System Safety Standardization Technical Committee.

1 Scope

This standard specifies the host file monitoring product safety function requirements, security requirements and classification requirements.

This standard applies to the host file monitoring 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 applies to this article Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Assessment Guidelines Part 3. Security components Information technology - Security terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 defined by the following terms and definitions apply to this document.

Hostfile hostsfile

Important system files, configuration files, and other predefined files stored on the host computer.

Host file monitoring hostsfilemonitoring Through the file integrity check, file attributes check, keyword checking and other means to modify the host file to monitor behavior.

User user

A person who has access to the host file and who does not have the authority to affect the execution of the host file monitoring security policy.

File monitoring security policy securitypolicyoffilemonitoring the detection of the host file, as well as the response to modify the behavior of the strategy set.

Authorized administrator Users who have the authority to manage the host file monitor

product are responsible for the system configuration, security policies, and audit logs in the product management.

4 Host file monitoring product description

Host file monitoring products based on pre-defined security policy, through the file integrity check, file attributes check, keyword check, etc.

Means to modify the status of host files (including important system files, configuration files, and other pre-defined files stored on the host), modify Behavior and other monitoring and alarm, so as to ensure that the host file resources are not unauthorized access and operation.