Chinastandards.org

ICS 35.240
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 910-2010

Replacing GA/T 910-2010

Information security technology - Security technical requirements for intranet-host monitoring products

信息安全技术 内网主机监测产品安全技术要求

(English Translation)

Issued on: March 3, 2020 **Implemented on: May 1, 2020**

Issued by: Ministry of Public Security

Preview: page 1 of 4 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-910-2010

Chinastandards.org

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Safety function requirements
4.1 Safety monitoring function
4.2 Safety control function
4.3 Component Security
4.4 Managed Host Management
4.5 Security Management
4.6 Audit function
5 Security requirements
5.1 Development
5.2 Guiding documents
5.3 Life Cycle Support
5.4 Test
5.5 Vulnerability assessment
6 Security classification and requirements
6.1 Classification
6.2 Safety function requirements
6.3 Safety assurance requirements

Foreword

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

This standard replaces GA/T 910-2010 "Information Security Technology Intranet Host Monitoring Product Security Technical Requirements", and GA/T 910-2010 the main technical changes compared to:2010 are as follows:

---Modified the requirements for classification, dividing the classification into basic and enhanced levels (see Chapter 6, Chapter 7 of the:2010 edition);

---Modified the safety function requirements to separate the monitoring function from the control function (see 4.1, 4:2, Chapter 4 of the:2010 edition);

Preview: page 2 of 4 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-910-2010

---Modified the safety guarantee requirements (see Chapter 5, Chapter 5 of the:2010 edition);

---Added print monitoring (see 4.1:7);

---Added host security policy monitoring and host security policy reinforcement (see 4.1:11, 4:2:7);

---Added the managed host management requirements (see 4.4):

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security:

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

This standard was drafted: Computer Information System Safety Product Quality Supervision and Inspection Center of the Ministry of Public Security:

1 Scope

This standard specifies the safety function requirements, safety assurance requirements and classification requirements of intranet host monitoring products:

This standard applies to the design, development and testing of internal network host monitoring products:

2 Normative references

The following documents are indispensable for the application of this document: For dated reference documents, only the dated version applies to this article Pieces: For undated references, the latest version (including all amendments) applies to this document:

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Assessment Criteria Part 3: Security Assurance Components GB/T 25069-2010 Information Security Technical Terms

3 Terms and definitions

The following terms and definitions defined in GB/T 18336.3-2015 and GB/T 25069-2010 apply to this document:

Controlled host

Intranet host to be monitored:

Intranet host monitoring product Products that monitor and/or control various activities on the controlled host:

Preview: page 3 of 4 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-910-2010

Non-authorizedinternetconnection the behavior of the internal network host without authorization to access the external network:

Externalinterface

Various interfaces for data interaction between the computer and the outside world:

4 Safety function requirements

4.1

Safety monitoring function

4.1.1

Online status monitoring the product should be able to monitor the following status of the intranet host:

a) The online status of the controlled host and the running status of the agent;

b) Set the proxy installation status of online hosts within the IP address range:

Preview: page 4 of 4 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-910-2010