ICS 35.240

A 90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

信息安全技术 网站监测产品安全技术要求

Information security technology Security technical requirements for website monitoring products

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 网站监测产品描述 1
6 总体说明 1
6.1 安全技术要求分类 2
6.2 安全等级 2
7 安全功能要求 2
7.1 HTTP 监测 2
7.2 支持 SSL 应用 2
7.3 PING 监测 2
7.4 业务流程监测 2
7.5 网站服务器监测 2
7.6 木马监测 2
7.7 敏感词信息监测 2
7.8 非法暗链监测 2
7.9 钓鱼监测 3
7.10 监测响应 3
7.11 监测结果处理 3
7.12 组件安全 3
7.13 远程管理 3
7.14 安全管理 4
7.15 自身审计功能 4
8 安全保障要求 5
8.1 开发 5
8.2 指导性文档 6
8.3 生命周期支持 6
8.4 测试 7
8.5 脆弱性评定 7
9 等级划分要求 7
9.1 概述 ..... **错误!未定义书签。**
9.2 安全功能要求等级划分 7

9.3 安全保障要求等级划分 8

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：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所、碁震（上海）云计算科技有限公司。

本标准主要起草人： 韦湘、赖静、俞优、沈亮、张笑笑、宋好好、王琦、王海兵。

信息安全技术 网站监测产品安全技术要求

1 范围

本标准规定了网站监测产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于网站监测产品的设计、开发与测试。

2 规范性引用文件

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

GB/T 25069－2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3－2015和GB/T 25069－2010界定的以及下列术语和定义适用于本文件。

3.1

网站监测产品 website monitoring product

具备持续的网站监测能力，并能配置响应策略对违反安全策略的异常情况进行实时告警的安全产品。

4 缩略语

下列缩略语适用于本文件。

HTTP：超文本传送协议 (HyperText Transfer Protocol)

SSL： 安全套接层(Secure Sockets Layer)

PING：因特网包探索器 (Packet Internet Groper)

5 网站监测产品描述

此类产品提供持续监测网站的功能，并能配置响应策略对违反安全策略的异常情况进行实时告警。

网站监测产品一般由网站监测管理组件、网站服务监测组件构成。网站监测管理端提供策略配置、监测结果响应等功能，网站服务监测组件对网站进行监测并上传监测信息到网站监测服务端；部分网站监测产品还提供网站服务器监测功能，需在网站服务器上安装客户端，通过客户端收集网站服务器的相关信息（如cpu、内存使用情况、服务器运行日志等）发送到网站监测服务器端。

6 总体说明

6.1 安全技术要求分类

本标准将网站监测产品安全技术要求分为安全功能、安全保障两个大类。其中，安全功能要求是对网站监测产品应具备的安全功能提出具体要求，包括HTTP监测、支持SSL应用、PING监测、监测结果响应等；安全保障要求为保障网站监测产品的生命周期过程而提出了具体要求，例如开发、指导性文档、生命周期支持和测试等。

6.2 安全等级划分

网站监测产品的安全等级按照其安全功能要求、自身安全功能要求和安全保障要求的强度划分为基本级和增强级，其中安全保障要求参考了GB/T 18336.3—2015。

7 安全功能要求

7.1 HTTP 监测

产品应支持配置安全策略对网站HTTP服务进行监测，对其是否可用、响应时间等指标进行监测。

7.2 支持 SSL 应用

产品应能对基于HTTPS协议的网站进行监测。

7.3 PING 监测

产品应支持配置安全策略对网站进行PING监测，并对其是否可用、响应时间以及丢包率等指标进行监测。

7.4 业务流程监测

产品应支持配置安全策略，模拟用户业务流程处理操作，对网站指定业务流程是否可用及其流程处理时间等指标进行监测。

7.5 网站服务器监测

产品应支持配置安全策略对网站服务器的运行状态进行监测:

a）监测内容应包括网站服务器CPU、内存、存储使用率以及网络流量等；

b）若网站服务器监测功能需在服务器上安装客户端，则客户端不应对网站服务器的正常运行产生明显影响。

7.6 木马监测

产品应支持配置安全策略，对被监测网站网页是否包含木马进行监测，包括：

a）静态木马监测方式：基于收集的木马特征库进行监测；

b）沙箱木马检测方式：基于沙箱技术进行动态监测。

7.7 敏感词信息监测

产品应支持自定义关键字策略，实时对目标站点页面是否出现关键词进行监测。

7.8 非法暗链监测

产品应支持配置安全策略，对网站隐藏的非法链接进行监测。

7.9 钓鱼监测

产品应支持配置网站钓鱼监测策略，对被监测网站是否被钓鱼进行监测。

7.10 监测响应

产品应具备下列监测响应功能：

a）对监测到的违反安全策略的事件进行实时告警，并支持用户自定义告警事件范围；

b）告警方式采用屏幕实时提示，E-mail告警、短信告警、声音告警等方式中的一种或多种；

c）告警信息至少包含事件日期、时间、事件描述等信息；

d）产品应具有对高频度发生的相同安全事件进行合并告警的能力。

7.11 监测结果处理

7.11.1 审计记录生成

产品应能将监测到的事件生成审计记录，并至少包含以下内容：日期、时间、主体信息、详细描述。

7.11.2 分析报表

产品应能根据日期、时间、事件类型、事件等级或其他审计信息生成监测结果分析报表，并能以通用格式输出。

7.11.3 审计记录存储

产品应采取以下措施防止审计记录丢失：

a）采取安全机制，保护审计记录免遭未经授权的读取、删除或修改；

b）审计记录应存储于掉电非易失性存储介质中，当审计记录的存储容量达到阈值时，产品应能发出报警信息；

c）产品应提供审计记录备份功能。

7.12 组件安全

7.12.1 组件状态监视

产品应支持对所有组件的运行状态进行监视，并在审计日志中记录所有组件状态的变更。

7.12.2 数据传输安全

若产品组件间通过网络进行通讯，产品应对组件间相互传输的数据进行保护，保证数据在传送过程中的保密性和完整性。

7.12.3 时间同步

产品应提供时间同步功能，保证产品组件之间时间的一致性。

7.13 远程管理

若产品提供远程管理功能，应对远程管理信息进行非明文传输。

7.14 安全管理

7.14.1 管理员属性初始化

产品应提供授权管理员属性的初始化能力。

7.14.2 管理员标识唯一

产品应为授权管理员提供唯一的身份标识，同时将授权管理员的身份标识与该授权管理员的所有可审计事件相关联。

7.14.3 管理员属性修改

产品应提供授权管理员的属性的修改能力。

7.14.4 管理角色

产品应能对管理员角色进行区分，自定义各种不同权限角色，并可对管理员分配角色。

7.14.5 身份鉴别

产品应在执行任何与安全功能相关的操作之前应鉴别任何声称要履行授权管理员职责的管理员身份。

7.14.6 鉴别失败处理

当对授权管理员鉴别失败的次数达到指定阈值后，产品应阻止授权管理员进一步的鉴别请求。

7.15 自身审计功能

7.15.1 审计日志生成

产品应能对下列事件生成审计日志：

a） 授权管理员鉴别成功和失败；

b） 管理员鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；

c） 管理员的重要操作，如新建、修改和删除安全策略；

d） 增加、删除管理员，备份日志等；

e） 组件状态变更；

f） 管理员的其它操作。

应在每一个审计日志中记录事件发生的日期和时间、事件主体身份、事件描述。

7.15.2 审计日志存储

产品应提供以下功能对审计日志进行存储:

a） 存储在掉电非易失性存储介质中；

b） 当存储空间达到阈值时，应能通知授权管理员。

7.15.3 审计日志管理

产品应提供以下功能对审计日志进行管理：

a） 授权管理员访问审计日志；

b） 使用时间、用户等条件对审计日志进行组合查询；

c） 日志进行备份及清空。

8 安全保障要求

8.1 开发

8.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a） 与产品设计文档中对安全功能实施抽象描述的级别一致；
b） 描述与安全功能要求一致的产品安全功能的安全域；
c） 描述产品安全功能初始化过程为何是安全的；
d） 证实产品安全功能能够防止被破坏；
e） 证实产品安全功能能够防止安全特性被旁路。

8.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a） 完全描述产品的安全功能；
b） 描述所有安全功能接口的目的与使用方法；
c） 标识和描述每个安全功能接口相关的所有参数；
d） 描述安全功能接口相关的安全功能实施行为；
e） 描述由安全功能实施行为处理而引起的直接错误消息；
f） 证实安全功能要求到安全功能接口的追溯；
g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

8.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

8.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a） 根据子系统描述产品结构；
b） 标识和描述产品安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其它模块间的相互作用；
h） 描述所有实现模块的安全功能要求相关接口、其它接口的返回值、与其它模块间的相互作用及调用的接口；

i） 描述所有安全功能的支撑或相关模块，包括其目的及与其它模块间的相互作用。

8.2 指导性文档

8.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所必须执行的安全策略。

8.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b） 描述安全安装产品及其运行环境必需的所有步骤。

8.3 生命周期支持

8.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a） 为产品的不同版本提供唯一的标识；
b） 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c） 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d） 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e） 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f） 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

8.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a） 产品、安全保障要求的评估证据和产品的组成部分；
b） 实现表示、安全缺陷报告及其解决状态。

8.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

8.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

8.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

8.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

8.4 测试

8.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

8.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

8.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其它测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期测试结果的一致性。

8.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

8.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；
b) 具有增强型基本攻击潜力的攻击者的攻击。

9 不同安全等级的要求

9.1 安全功能要求

不同安全等级的网站监测产品的安全功能如表 1 所示。

表 1 不同安全等级的网站监测产品的安全功能要求

安全功能要求		基本级	增强级
HTTP 监测		7.1	7.1
支持 SSL 应用		7.2	7.2
PING 监测		7.3	7.3
业务流程监测		——	7.4
网站服务器监测		7.5	7.5
木马监测		7.6	7.6
敏感词信息监测		7.7	7.7
非法暗链监测		7.8	7.8
钓鱼监测		——	7.9
监测响应		7.10 a）～c）	7.10
监测结果处理	审计记录生成	7.11.1	7.11.1
	分析报表	7.11.2	7.11.2
	审计记录存储	7.11.3	7.11.3
组件安全	组件状态监视	7.12.1	7.12.1
	数据传输安全	7.12.2	7.12.2
	时间同步	7.12.3	7.12.3
远程管理		7.13	7.13
安全管理	管理员属性初始化	7.14.1	7.14.1
	管理员唯一性标识	7.14.2	7.14.2
	管理员属性修改	7.14.3	7.14.3
	管理角色	——	7.14.4
	身份鉴别	7.14.5	7.14.5
	鉴别失败处理	——	7.14.6
自身审计功能	审计日志生成	7.15.1	7.15.1
	审计日志存储	7.15.2	7.15.2
	审计日志管理	7.15.3	7.15.3

9.2 安全保障要求

不同安全等级的网站监测产品的安全保障要求如表 2 所示。

表 2 不同安全等级的网站监测产品的安全保障要求

安全保障要求		基本级	增强级
开发	安全架构	8.1.1	8.1.1

表 2 （续）

安全保障要求		基本级	增强级
开发	功能规范	8.1.2 a) ～f)	8.1.2
	实现表示	——	8.1.3
	产品设计	8.1.4 a) ～d)	8.1.4
指导性文档	操作用户指南	8.2.1	8.2.1
	准备程序	8.2.2	8.2.2
生命周期支持	配置管理能力	8.3.1 a) ～c)	8.3.1
	配置管理范围	8.3.2 a)	8.3.2
	交付程序	8.3.3	8.3.3
	开发安全	——	8.3.4
	生命周期定义	——	8.3.5
	工具和技术	——	8.3.6
测试	覆盖	8.4.1 a)	8.4.1
	深度	——	8.4.2
	功能测试	8.4.3	8.4.3
	独立测试	8.4.4	8.4.4
脆弱性评定		8.5 a)	8.5