ICS 35.240
A90

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 工业控制系统软件脆弱性扫描产品安全技术要求

Information security technology Security technical requirements for industrial control system software vulnerability scanners

（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

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。

本标准主要起草人：李曦、沈清泓、俞优、邹春明、陆臻、顾健。

信息安全技术 工业控制系统软件脆弱性扫描产品安全技术要求

1 范围

本标准规定了工业控制系统软件脆弱性扫描产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于工业控制系统软件脆弱性扫描产品的设计、开发和测试。

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 第3部分：安全保障组件

GB/T 25069-2010 信息安全技术 术语

GB/T 30976.1-2014工业控制系统信息安全 第1部分：评估规范

3 术语和定义

GB/T 25069-2010和GB/T 30976.1-2014界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统软件 industrial control system software

工业控制系统上位机软件和下位机软件的集合。

3.2

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安全策略。

3.3

旗标 banner

由应用程序发送的一段信息，通常包括欢迎语、应用程序名称和版本等信息。

4 缩略语

下列缩略语适用于本文件。

DCS：集散控制系统（Distributed Control System）

HMI：人机接口（Human Machine Interface）

PLC：可编程逻辑控制器（Programmable Logic Controller）

SCADA：数据采集与监控系统（Supervisory Control And Data Acquisition）

5 总体说明

5.1 安全技术要求分类

本标准将工业控制系统软件脆弱性扫描产品安全技术要求分为安全功能和安全保障要求。其中，安全功能要求是对工业控制系统软件脆弱性扫描产品应具备的安全功能提出具体要求，通过一定的用户标识和鉴别来限制对产品功能的使用和数据访问的控制，使产品具备自主安全保护的能力，保证工业控制系统软件脆弱性扫描产品的正常运行，具备审计功能要求，使得管理员的各项操作行为和扫描事件都是可追踪的。安全保障要求针对工业控制系统软件脆弱性扫描产品的开发和使用文档的内容提出具体的要求，例如开发、测试和指导性文档等。

5.2 安全等级划分

工业控制系统软件脆弱性扫描产品的安全等级按照其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。

6 安全功能要求

6.1 信息获取

6.1.1 支撑系统信息

应能对工业控制系统软件所在支撑平台的操作系统类型、版本号进行探测，能够获取已开启的各项TCP/IP服务的旗标。

6.1.2 开放端口

应能探测到工业控制系统软件所在操作系统开放的TCP、UDP端口，并能判断相应端口对应的通用服务或使用的协议

6.1.3 协议支持

应能支持典型工业控制协议，如MODBUS TCP、OPC、西门子S7、IEC 60870-5-104、IEC61850等。

6.2 脆弱性扫描内容

6.2.1 漏洞发现

应能发现公开的工业控制系统软件的安全脆弱性问题。

6.2.2 漏洞挖掘

应能发现未知的工业控制系统软件的安全脆弱性问题。

6.2.3 弱口令

应能采用字典或穷举等方法检查系统用户口令的健壮性，检查项目应包括：

a) 系统是否使用了用户名称经过简单变换后的口令；
b) 系统是否使用了易猜测口令。

6.2.4 文件共享

应能检查文件共享机制，发现危险的设置，检查项目应包括：

a） 重要目录被共享；

b） 共享目录可被匿名用户写入；

c） 是否使用了缺省或过于简单的共享口令。

6.3 扫描结果分析处理

6.3.1 扫描结果浏览及导出

应提供扫描结果浏览功能，并支持对扫描结果数据进行导出操作。

6.3.2 报告生成

能根据扫描结果生成相应的报告，报告具备要求包括如下内容：

a) 各脆弱点的漏洞名称、漏洞描述、影响范围等；

b) 目标的风险等级评估，将扫描脆弱点按风险严重程度分级，并明确标出；

c) 多个目标扫描后的结果的总体报告；

d) 对脆弱性扫描信息可生成摘要报告；

e) 应可输出为通用的文档格式。

6.3.3 报告定制

应提供报告内容定制功能。

6.3.4 脆弱性修补建议

能对发现的脆弱性提出修补建议，脆弱性修补建议满足下列要求：

a） 对不同的安全脆弱性问题提出针对性的脆弱性修补方法；

b） 脆弱性描述应详细，提供的脆弱性修补方法应确保其合理性和可用性。

6.3.5 结果比对

应提供对同一目标多次扫描结果或者不同主机间扫描结果的比对功能，并能根据比对结果生成比对报告。

6.4 扫描配置

6.4.1 扫描策略

应提供方便的定制策略的方法，可以指定扫描地址范围、端口范围、脆弱性类型等。

6.4.2 向导功能

应提供向导功能，方便用户进行扫描策略配置。

6.4.3 计划任务

应能定制扫描计划，可以定时启动或者按周期执行扫描任务。

6.4.4 已知账号/口令扫描

应能使用目标系统的已知账号/口令对其进行更有效的扫描。

6.5 目标对象的安全性

应支持以下方式，避免影响目标对象及其所在网络的正常工作：

a) 支持采用版本探测与漏洞库比对方式进行扫描，避免漏洞验证方式对系统的影响；

b) 通过调整扫描线程、进程数目或请求数量等方法，提供合理的扫描速度。

6.6 升级能力

应能够对脆弱性特征库进行更新：

a) 支持手动或者自动升级操作；

b) 具备升级安全措施。

6.7 扫描 IP 地址限制

应提供对产品扫描范围进行限制的手段。

6.8 自身安全要求

6.8.1 标识和属性

6.8.1.1 唯一性标识

应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计能力相关联。

6.8.1.2 属性定义

应为每个管理角色规定与之相关的安全属性，例如管理角色标识、鉴别信息、隶属组、权限等。

6.8.1.3 属性初始化

应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

6.8.2 身份鉴别

6.8.2.1 基本鉴别

应在执行任何与管理员相关功能之前鉴别用户的身份。

6.8.2.2 鉴别数据保护

应保证鉴别数据不被未授权查阅或修改。

6.8.2.3 鉴别失败处理

应提供一定的鉴别失败处理措施，当鉴别失败次数达到设定值时，应能阻止该用户的进一步鉴别尝试。

6.8.2.4 超时锁定或注销

应具有登录超时锁定或注销功能，在设定的时间段内没有任何操作的情况下，能锁定或终止会话，需要再次进行身份鉴别才能重新操作，最大超时时间仅由授权管理员设定。

6.8.3 安全管理

6.8.3.1 安全管理功能

应保证授权管理员具备以下管理权限：

a） 查看安全属性；

b） 修改安全属性；

c） 启动、关闭全部或部分安全功能；

d） 制定和修改各种安全策略。

6.8.3.2 角色管理

能对管理员角色进行区分：

a） 具有至少两种不同权限的管理员角色，如操作员、安全员、审计员等；

b） 应根据不同的功能模块，自定义各种不同权限角色，并可对管理员分配角色。

6.8.3.3 远程安全管理

若产品提供远程管理功能：

a） 应能保护远程管理对话内容不被非授权获取；

b） 应能对可远程管理的主机地址进行限制。

6.8.4 审计日志

6.8.4.1 审计日志生成

应能对以下事件生成日志：

a） 管理员的登录成功和失败；

b） 对安全策略进行更改的操作；

c） 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；

d） 对管理员、管理角色进行增加、删除和属性修改的操作；

e） 对审计日志的导出和删除操作；

f） 扫描任务的启动、暂停和停止等操作。

每一条审计日志中至少应包括事件主体、事件发生的日期、时间，事件描述和结果。若采用远程登录方式对产品进行管理还应记录管理主机的地址。

6.8.4.2 审计日志保存

审计日志应能存储于掉电非易失介质中。

6.8.4.3 审计日志管理

提供下列审计日志管理功能：

a） 只允许授权管理员访问审计日志；

b） 提供对审计日志的查询功能；

c） 授权管理员应能导出审计日志；

d） 提供对审计日志的按条件查询和排序功能。

6.8.4.4 审计存储安全

应提供数据存储空间耗尽处理功能，当剩余存储空间达到阈值时，提供告警功能。

7 安全保障要求

7.1 开发

7.1.1 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。

7.1.2 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。

7.1.3 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。

7.1.4 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，包括其目的及与其他模块间的相互作用；
h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他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，包括其目的及与其他模块间的相互作用。

7.2 指导性文档

7.2.1 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需执行的安全策略。

7.2.2 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。

7.3 生命周期支持

7.3.1 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。

7.3.2 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。

7.3.3 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。

7.3.4 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。

7.3.5 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。

7.3.6 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。

7.4 测试

7.4.1 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。

7.4.2 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。

7.4.3 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他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的测试结果的一致性。

7.4.4 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。

7.5 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。

8 不同安全等级的要求

8.1 安全功能要求

不同安全等级的工业控制系统软件脆弱性扫描产品的安全功能要求如表1所示。

表1 不同安全等级的工业控制系统软件脆弱性扫描产品的安全功能要求

安全功能要求		基本级	增强级
信息获取	支撑系统信息	6.1.1	6.1.1

表1 （续）

安全功能要求		基本级	增强级
信息获取	开放端口	6.1.2	6.1.2
	协议支持	6.1.3	6.1.3
脆弱性扫描内容	漏洞发现	6.2.1	6.2.1
	漏洞挖掘	——	6.2.2
	弱口令	6.2.3	6.2.3
	文件共享	6.2.4	6.2.4
扫描结果分析处理	扫描结果浏览及导出	6.3.1	6.3.1
	报告生成	6.3.2	6.3.2
	报告定制	——	6.3.3
	脆弱性修补建议	6.3.4	6.3.4
	结果比对	——	6.3.5
扫描配置	扫描策略	6.4.1	6.4.1
	计划任务	6.4.2	6.4.2
	已知账号/口令扫描	——	6.4.3
目标对象的安全性		6.5	6.5
升级能力		6.6 a)	6.6
扫描 IP 地址限制		——	6.7
自身安全要求	标识和属性	6.8.1	6.8.1
	身份鉴别	6.8.2	6.8.2
	安全管理	6.8.3.1、6.8.3.3 a)、6.12.3.4 a)	6.8.3
	审计日志	6.8.4.1-6.8.4.3	6.8.4

8.2 安全保障要求

不同安全等级的工业控制系统软件脆弱性扫描产品的安全保障要求如表 2 所示。

表2 不同安全等级的工业控制系统软件脆弱性扫描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	7.1.1	7.1.1
	功能规范	7.1.2 a) ～f)	7.1.2
	实现表示	——	7.1.3
	产品设计	7.1.4 a) ～d)	7.1.4
指导性文档	操作用户指南	7.2.1	7.2.1
	准备程序	7.2.2	7.2.2
生命周期支持	配置管理能力	7.3.1 a) ～c)	7.3.1
	配置管理范围	7.3.2 a)	7.3.2

表2 （续）

安全保障要求		基本级	增强级
生命周期支持	交付程序	7.3.3	7.3.3
	开发安全	——	7.3.4
	生命周期定义	——	7.3.5
	工具和技术	——	7.3.6
测试	测试覆盖	7.4.1 a)	7.4.1
	测试深度	——	7.4.2
	功能测试	7.4.3	7.4.3
	独立测试	7.4.4	7.4.4
脆弱性评定		7.5 a)	7.5 b)