ICS 35.080
L 77

中华人民共和国国家标准

GB/T 34943—2017

C/C++语言源代码漏洞测试规范

Source code vulnerability testing specification for C/C++

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:珠海南方软件网络评测中心、珠海中慧微电子有限公司、广东省科技基础条件平台中心、中国电子技术标准化研究院、上海端玛计算机科技有限公司、南昌金庐软件园软件评测培训有限公司、国家应用软件产品质量监督检验中心、珠海市软件行业协会、东信和平科技股份有限公司、南京大学。

本标准主要起草人:侯建华、邓人逖、王忠福、黄兆森、杨尚沅、张旸旸、赵昌平、张子良、李璐、肖枭、陈振宇、张玉霞、梁建新、蒋蜀鹏、周悦、任佩、杨雪君。

引　言

C 语言是一种面向过程的程序设计语言，广泛应用于系统软件与嵌入式软件的开发。本标准的 C 语言语法遵循 ISO/IEC 9899:2011。C++语言是一种面向对象的程序设计语言，它在 C 语言的基础上发展而来，与 C 语言具有许多相同的语法，广泛应用于系统软件与应用软件的开发。本标准的 C++语言语法遵循 ISO/IEC 14882:2011 语法标准。众所周知，由于各种人为因素影响，每个软件的源代码都难免会存在漏洞，而软件信息泄露、数据或代码被恶意篡改等安全事件的发生一般都与源代码漏洞有关。为尽量减少 C/C++语言源代码中存在的漏洞，有必要制定针对 C/C++语言程序的源代码漏洞测试规范。

源代码漏洞测试可在开发过程的软件编码活动之后实施，也可在运行和维护过程中实施。

本标准的漏洞分类与漏洞说明主要参考了 MITRE 公司发布的 CWE(Common Weakness Enumeration)，同时结合了当前行业主流的自动化静态分析工具在测试实践中发现的典型漏洞来确定并进行说明。

注：本标准漏洞参考了 CWE2.9 版本，示例代码适用于本标准选择的案例。

本标准仅针对自动化静态分析工具支持的关键漏洞进行说明，应用本标准开展源代码漏洞测试时应根据实际需要对漏洞进行裁剪和补充。

C/C++语言源代码漏洞测试规范

1 范围

本标准规定了C/C++语言源代码漏洞测试的测试总则和测试内容。

本标准适用于开发方或第三方机构的测试人员利用自动化静态分析工具开展的C/C++语言源代码漏洞测试活动，C/C++语言的程序设计和编码人员以及源代码漏洞测试工具的设计人员也可参考使用。

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 11457 信息技术 软件工程术语

GB/T 15532—2008 计算机软件测试规范

GB/T 20158—2006 信息技术 软件生存周期过程 配置管理(ISO/IEC TR 15846:1998,IDT)

3 术语和定义

GB/T 11457界定的以及下列术语和定义适用于本文件。

3.1

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[GB/T 25069—2010,定义 2.2.1.42]

3.2

攻击 attack

在信息系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能的尝试(包括窃取数据)。

[GB/T 25069—2010,定义 2.2.1.58]

3.3

密码分组链接 cipher block chaining

对信息加密时，每一密文块在加密时都依赖于前一密文块的方式。

3.4

密文 ciphertext

利用加密技术，经变换，信息内容被隐藏起来的数据。

[GB/T 25069—2010,定义 2.2.2.105]

3.5

解密 decryption

将密文转换为明文的处理，即加密对应的逆过程。

[GB/T 25069—2010,定义 2.2.2.69]