Q/PL

凭 阑 实 验 室 企 业 标 准

Q/PL 001-2024

CNCVE 漏洞编号及属性规范

2024-01-01 发布　　2024-01-01 实施

凭阑江苏实验室科技有限公司　发布

目　次

前　言

为规范 CNCVE 漏洞管理工作，根据凭阑实验室质量管理体系要求，特制定本标准。
本标准按照 GB/T1.1-2020 给出的规则起草。
本标准由凭阑江苏实验室科技有限公司提出并归口。
本标准起草单位：凭阑江苏实验室科技有限公司。
本标准主要起草人：吴青松。

CNCVE 漏洞编号及属性规范

1 范围

本标准规定了CNCVE漏洞编号及属性规范。

本标准适用于CNCVE中文漏洞知识库平台产品的设计开发与兼容性使用。

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，仅所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 25069 信息安全技术 术语

GB/T 28458 信息安全技术 安全漏洞标识与描述规范

GB/T 30276 信息安全技术 信息安全漏洞管理规范

GB/T 30279 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 漏洞 vulnerability

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

4 缩略语

下列缩略语适用于本文件。

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

NVDB：网络安全威胁和漏洞信息共享平台（National Vulnerability DataBase）

CVE：通用漏洞披露（Common Vulnerabilities & Exposures）

5 CNCVE 概述

中文漏洞知识库（Chinese Common Vulnerabilities and Exposures，简称“CNCVE”），是凭阑实验室基于公开漏洞进行收集、分析和评估，负责运营的中文信息安全漏洞知识管理平台，旨在为全球信息安全保障提供服务。通过社区建设与运营，CNCVE 在信息安全漏洞搜集、重大漏洞信息通报、高危漏洞安全消控等方面发挥了重大作用，为全球重要行业和关键设施安全保障工作提供了重要的技术支撑和数据支持。

6 CNCVE 漏洞规范

5.1 漏洞编号规则

“漏洞编号”是用来对每个漏洞进行唯一标识的代码,其格式为:CNCVE-N^+-YYYY，如图 1 所示：

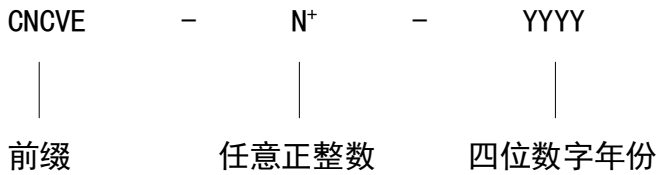

图 1 CNCVE 漏洞编号规则

其中，CNCVE 为固定编码前缀；N^+为多位十进制正整数数字序列号，从“1”开始编号；YYYY 为 4 位十进制数字，表示漏洞发现的年份。

5.2 漏洞属性字段

除了漏洞编号，漏洞字段还包括名称、发布时间、发布者、验证者、发现者、类别、等级、受影响产品或服务、相关编号、存在性说明等必须项，并可根据需要扩展检测方法、解决方案、其他描述等扩展项，扩展项为可选。

表 1 CNCVE 漏洞属性字段

字段名称	描述
漏洞名称	概括性描述漏洞信息的短语。
漏洞编号	CNCVE 对每个漏洞进行唯一标识的代码。
CVE 编号	该漏洞被 CVE 收录赋予的编号。
CNVD 编号	该漏洞被 CNVD 收录赋予的编号。
CNNVD 编号	该漏洞被 CNNVD 收录赋予的编号。
NVDB 编号	该漏洞被 NVDB 收录赋予的编号。
其他相关编号	同一漏洞在不同组织中的编号（不含以上四个组织），若存在多个编号可顺序给出，中间以逗号分隔。
公开日期	漏洞信息公开披露的日期。日期格式为：YYYY-MM-DD，如 2024-01-01。
危害级别	分为超危、高危、中危、低危四种级别。
漏洞评分	参照 CVSS 规范，分为 CVSS4.x、CVSS3.x、CVSS2.x 三种评分方法，给出三种评分结果。
影响产品	参照 CPE 规范，指漏洞所存在的产品或服务的详细信息，包括供应商、名称,版本号等内容。对于共用中间件或者组件的漏洞,受其影响的相关产品或服务信息均可列出。
漏洞描述	漏洞详细信息。
漏洞类型	参照 CWE 规范，包括 CWE-ID 及 CWE 名称。
参考链接	其他平台针对该漏洞的描述，一般是漏洞的来源信息或参考信息。
漏洞解决方案	漏洞的解决方案，例如补丁信息、修复或防范措施等。
厂商补丁	厂商针对该漏洞发布的最新补丁信息。
验证信息	验证状态，包括已验证或未验证。新报送的漏洞需首先进行验证。
漏洞状态	状态包括保留、争议、拒绝、发布等，未通过验证的漏洞无状态信息。
贡献者	发现漏洞信息的个人或组织。
贡献者单位	贡献者的工作单位名称。
报送时间	漏洞信息报送日期，日期格式为：YYYY-MM-DD。
收录时间	漏洞信息被正式收录日期，日期格式为：YYYY-MM-DD。
更新时间	漏洞信息更新日期，日期格式为：YYYY-MM-DD。
漏洞附件	涉及该漏洞的相关文档。