奥邦检验认证集团有限公司企业标准

CTS_ABG 69147-2024

网络安全漏洞披露管理体系 要求

Cybersecurity vulnerability disclosure management systems - Requirements

2024-06-28 发布　　**2024-06-28** 实施

奥邦检验认证集团有限公司 发布

目录

前言

本标准按照 GB/T1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本标准依据相关标准化规则制定，旨在为组织建立、实施、维护和持续改进网络安全漏洞披露管理体系提供全面且规范的要求。通过明确漏洞披露各环节的流程、职责和控制措施，助力组织有效管理网络安全漏洞信息，降低安全风险，保障信息系统的安全稳定运行。

在标准制定过程中，充分参考了国内外相关法律法规、行业最佳实践以及现有网络安全标准，力求使本标准具有科学性、实用性和前瞻性。

本标准的发布实施，将有助于统一网络安全漏洞披露管理的行业规范，提升组织应对网络安全威胁的能力，促进网络安全生态的健康发展。

本标准所规定的网络安全漏洞披露管理体系，强调基于风险管理的理念，通过建立完善的流程和控制机制，实现对漏洞从发现、报告、评估、处置到跟踪反馈的全生命周期管理。同时，注重与其他信息安全管理体系的兼容性和协同性，以保障组织整体信息安全目标的实现。

本标准主要起草人：袁海、邵优良。

本标准由奥邦检验认证集团有限公司 2024 年 06 月 28 日批准发布。

本标准自 2024 年 06 月 28 日发布之日起起实施。

本标准由奥邦检验认证集团有限公司解释。

网络安全漏洞披露管理体系 要求

1.范围

本标准明确规定了网络安全漏洞披露管理体系的要求，适用于各类希望建立、实施、维护和持续改进漏洞披露管理能力的组织，无论其规模大小、行业类型和业务性质如何。

组织在应用本标准时，应确保覆盖所有与网络安全漏洞披露相关的活动、流程和人员，包括但不限于漏洞发现者、报告者、接收者、评估者、处置者以及相关管理层。

本标准可作为组织内部自我评估和改进的依据，也可用于外部各方对组织网络安全漏洞披露管理能力的评价和审核。

2.规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 29246-2023《信息技术 安全技术 信息安全管理体系 概述和词汇》

GB/T 30276-2020《信息安全技术 网络安全漏洞管理规范》

ISO/IEC 29147:2018《信息技术-安全技术 漏洞披露》

3.术语和定义

为确保本标准的准确理解和有效实施，对以下关键术语进行定义：

3.1 网络安全漏洞：信息系统在硬件、软件、协议的设计、实现或配置过程中存在的缺陷或弱点，可被利用以破坏系统的保密性、完整性或可用性。

3.2 漏洞披露：将网络安全漏洞相关信息，包括漏洞的发现情况、技术细节、影响范围等，按照规定的流程和方式，向特定的对象或公众进行通报的行为。

3.3 漏洞发现者：通过技术手段或其他途径，首次识别出网络安全漏洞存在的个人或组织。

3.4 漏洞报告者：将所发现的网络安全漏洞信息，按照规定的报告流程和格式，提交给指定接收方的个人或组织。

3.5 漏洞接收者：负责接收网络安全漏洞报告，并对报告进行初步处理和分类的组织或机构。

3.6 漏洞评估者：运用专业知识和工具，对网络安全漏洞的严重程度、影响范围、利用难度等进行分析和评价的个人或团队。

3.7 漏洞处置者：根据漏洞评估结果，负责制定和实施漏洞修复方案，降低漏洞风险的组织或部门。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。