汉坤法律评述

2021 年 7 月 15 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

《网络产品安全漏洞管理规定》简评

作者：段志超 | 解石坡

本周一（2021 年 7 月 12 日），工业和信息化部（“**工信部**”）、国家互联网信息办公室（“**网信办**”）和公安部联合发布了《网络产品安全漏洞管理规定》（“**《漏洞管理规定》**”），自 2021 年 9 月 1 日起施行，为网络安全监管这一近期备受关注的领域再添新规。

根据《漏洞管理规定》，网信办将负责统筹协调网络产品安全漏洞管理工作，工信部负责网络产品安全漏洞综合管理，并承担电信和互联网行业网络产品安全漏洞监督管理，而公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。

《漏洞管理规定》适用于网络产品（包括硬件和软件产品）提供者，网络运营者，从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，规定了这三类主体的法律义务和违法后果。同时，其要求其他组织或个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息，并且不得为利用网络产品安全漏洞从事危害网络安全的活动的主体提供技术支持、广告推广、支付结算等帮助。

鉴于网信办近日颁布了《网络安全审查办法》（修订草案征求意见稿）,其中强调了网络安全审查申报制度（汉坤此前的分析请见*《网络安全审查办法》（修订草案征求意见稿）快评*）对数据处理活动相关的数据泄露、窃取、毁损的风险的考量，《漏洞管理规定》的相关规定将对相关企业针对网络安全审查进行内部自查和对标具有较强的参考作用。

下表是本所对《漏洞管理规定》对于不同适用主体的有关规定的总结：

适用主体	鼓励事项	法律义务	违法后果
网络产品提供者	建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。	■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 发现或者获知所提供网络产品存在安全漏洞后，应当立即组织验证，评估危害程度和影响范围，及时组织修补漏洞； ■ 在 2 日内向工信部网络安全威胁和漏洞信息共享平台报送相关漏洞信息； ■ 对属于其上游产品或者组件存在的安全漏洞，应当立即通知相关产品提供者； ■ 对于需要产品用户（含下游厂商）采取软件、固件升级等措施的，应当及时告知漏洞风险及修补方式，并提供技术支持。	■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 5-50 万元罚款； ■ 对直接负责的主管人员处 1-10 万元罚款。
网络运营者		■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时进行验证并完成修补。	一般网络运营者： ■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 1-10 万元罚款； ■ 对直接负责的主管人员处 5,000 元-5 万元罚款； 关键信息基础设施的运营者： ■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 10-100 万元罚款； ■ 对直接负责的主管人员处 1-10 万元罚款。
从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人		■ 设立网络产品安全漏洞收集平台，应当向工业和信息化部备案； ■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 加强内部管理，采取措施防范漏洞信息泄露和违规发布； ■ 通过网络平台、媒体、会议、竞赛等方式向社会发布漏洞信息的，应当遵循必要、真实、客观以及有利于防范网络安全风险的原则； ■ 不得在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞	■ 责令改正，给予警告； ■ 拒不改正或者情节严重的，处 1-10 万元罚款； ■ 可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照； ■ 对直接负责的主管人员和其他直接责任人员处 5,000 元-5 万元罚款。

适用主体	鼓励事项	法律义务	违法后果
		信息；认为有必要提前发布的，应当与相关网络产品提供者共同评估协商，并向工信部、公安部报告，由工信部、公安部组织评估后进行发布； ■ 不得发布网络运营者在用的网络、信息系统及其设备存在安全漏洞的细节情况； ■ 不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动； ■ 不得发布或者提供专门用于利用网络产品安全漏洞从事危害网络安全活动的程序和工具； ■ 在发布网络产品安全漏洞时，应当同步发布修补或者防范措施； ■ 在国家举办重大活动期间，未经公安部同意，不得擅自发布网络产品安全漏洞信息； ■ 不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。	
其他组织或个人	■ 向网络产品提供者通报其产品存在的安全漏洞； ■ 向工信部网络安全威胁和漏洞信息共享平台、国家网络与信息安全信息通报中心漏洞平台、国家计算机网络应急技术处理协调中心漏洞平台、中国信息安全测评中心漏洞库报送网络产品安全漏洞信息。	■ 不得利用网络产品安全漏洞从事危害网络安全的活动； ■ 不得非法收集、出售、发布网络产品安全漏洞信息； ■ 明知他人利用网络产品安全漏洞从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。	**尚不构成犯罪的：** ■ 没收违法所得，处 5 日以下拘留；可以并处 5-50 万元罚款； ■ 情节较重的，处 5-15 日拘留；可以并处 10-100 万元罚款。 **单位有前款行为的：** ■ 没收违法所得； ■ 处 10-100 万元罚款； ■ 并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 **相关人员：** ■ 受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作； ■ 受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

解石坡

电话： +86 10 8524 5866
Email： angus.xie@hankunlaw.com