国盟信息安全通报

2019 年 8 月 05 日第 198 期

国盟信息安全通报

（第 198 期）

国际信息安全学习联盟

2019 年 8 月 05 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 443 个，其中高危漏洞 198 个、中危漏洞 181 个、低危漏洞 64 个。漏洞平均分值为 6.50。本周收录的漏洞中，涉及 0day 漏洞 107 个（占 24%），其中互联网上出现“Invoxia NVX220 信任管理问题漏洞、Private Internet Access (PIA) VPN 客户端任意代码执行漏洞（CNVD-2019-24214）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2259 个，与上周（3226 个）环比下降 30%。

主要内容

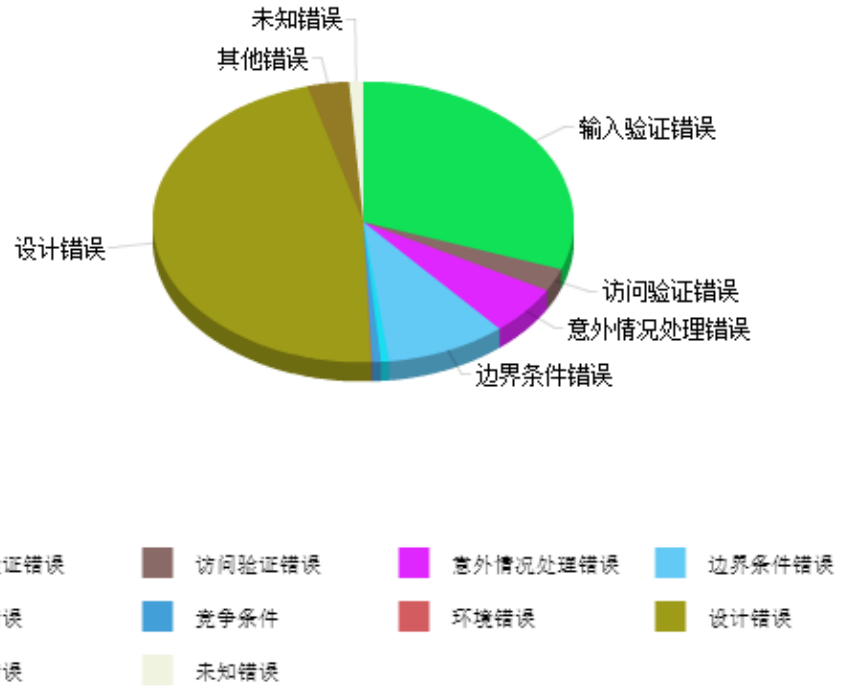
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

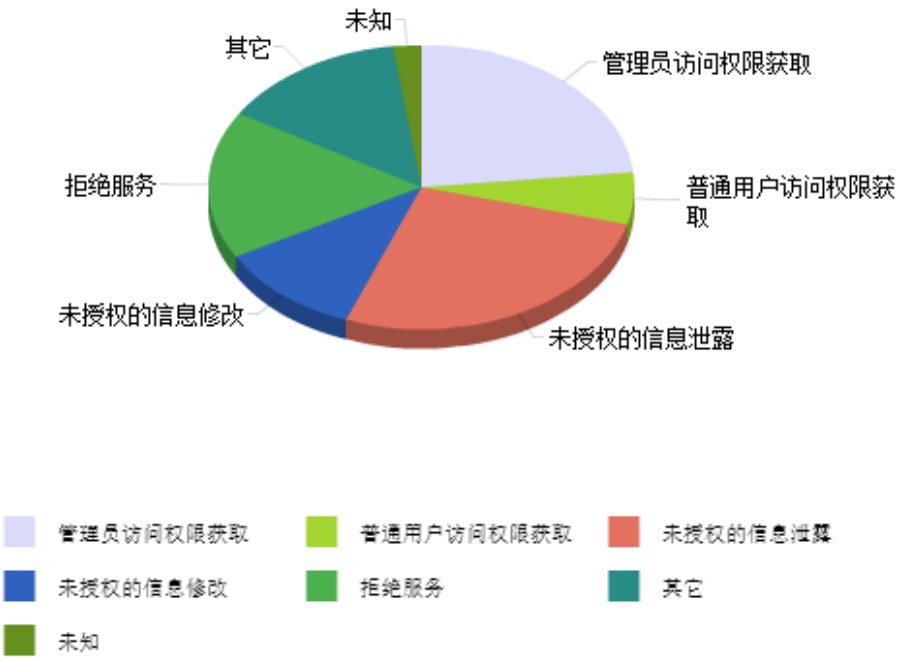
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 443 个，其中高危漏洞 198 个、中危漏洞 181 个、低危漏洞 64 个。漏洞平均分值为 6.50。本周收录的漏洞中，涉及 0day 漏洞 107 个（占 24%），其中互联网上出现“Invoxia NVX220 信任管理问题漏洞、Private Internet Access (PIA) VPN 客户端任意代码执行漏洞（CNVD-2019-24214）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2259 个，与上周（3226 个）环比下降 30%。

二、安全漏洞增长数量及种类分布情况

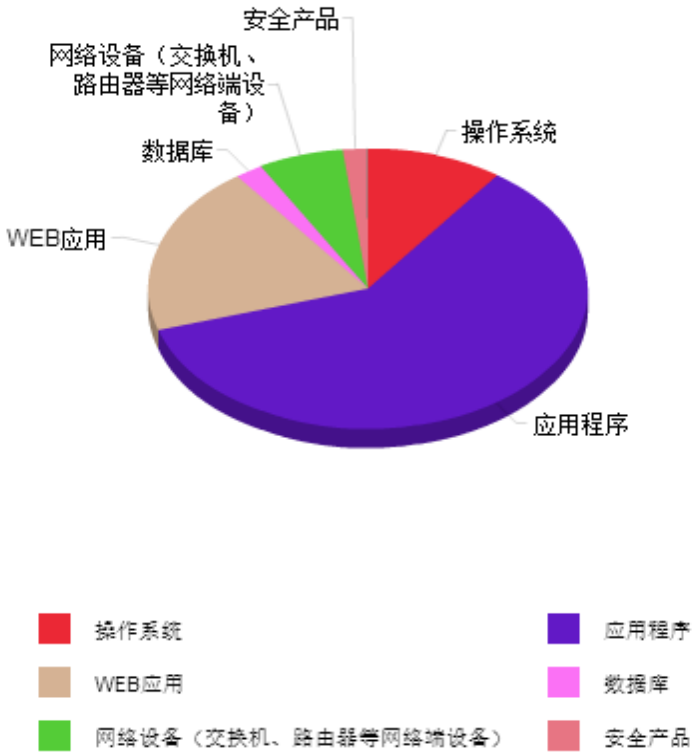
➢ 漏洞产生原因（2019 年 7 月 22 日—2019 年 8 月 05）



➢ 漏洞引发的威胁（2019 年 7 月 22 日—2019 年 8 月 05）



➢ 漏洞影响对象类型（2019 年 7 月 22 日—2019 年 8 月 05）



三、安全产业动态

➢ 中国国防白皮书发布：网络空间上升为国家主权的新疆域

2019 年 7 月 24 日，国务院新闻办公室正式发表《新时代的中国国防》白皮书，这是中国政府自 1998 年以来发表的第 10 部国防白皮书，也是党的十八大以来发表的首部综合型国防白皮书。发表国防白皮书的目的，是为了阐释新时代中国防御性国防政策，向国际社会更好地介绍中国建设巩固国防和强大军队的实践、目的、意义，增进国际社会对中国国防的理解，增进中国同世界各国的互信与合作。

《新时代的中国国防》白皮书分为前言、正文、结束语和附录四个部分，共约 2.7 万字。正文包括国际安全形势、新时代中国防御性国防政策、履行新时代军队使命任务、改革中的中国国防和军队、合理适度的国防开支、积极服务构建人类命运共同体等 6 个章节。附录包括 10 个表格，主要介绍军委机关部门基本情况、中国国防费规模结构、2012 年以来解放军和武警部队对外开展的主要联演联训活动、中国军队参加的主要联合国维和行动情况等。

《新时代的中国国防》白皮书正文的主要内容包括六个方面：

第一，客观分析当前的国际安全形势和中国安全环境。白皮书指出，当今世界正经历百年未有之大变局，世界面临的不稳定性不确定性更加突出，国际战略竞争呈上升之势，全球和地区性安全问题持续增多，国际军事竞争日趋激烈，世界并不太平。但必须看到，促和平、求稳定、谋发展已成为国际社会的普遍诉求，和平力量的上升远远超过战争因素的增长，和平、发展、合作、共赢的时代潮流不可逆转。白皮书同时指出，中国国家安全形势总体稳定，

但面临着多元复杂的安全威胁和挑战，特别是反分裂斗争形势更加严峻。

第二，系统阐述新时代中国防御性国防政策。白皮书强调，坚决捍卫国家主权、安全、发展利益是新时代中国国防的根本目标，坚持永不称霸、永不扩张、永不谋求势力范围是新时代中国国防的鲜明特征，贯彻落实新时代军事战略方针是新时代中国国防的战略指导，坚持走新时代中国特色强军之路是新时代中国国防的发展路径，服务构建人类命运共同体是新时代中国国防的世界意义。

第三，全面介绍中国军队履行新时代使命任务情况。白皮书明确中国军队新时代的使命任务是“四个战略支撑”，从维护国家领土主权和海洋权益、保持常备不懈的战备状态、开展实战化军事训练、维护重大安全领域利益、遂行反恐维稳、维护海外利益、参加抢险救灾等 7 个方面介绍了中国武装力量运用情况。

第四，全景式介绍深化国防和军队改革取得的历史性成就。白皮书系统介绍中国军队重塑领导指挥体制、优化规模结构和力量编成、推进军事政策制度改革的有关情况，全面介绍调整改革后的军兵种和武警部队基本情况，以及思想政治、军事理论、武器装备、后勤保障等国防和军队全面建设情况，展示改革后中国军队的崭新形象。

第五，多维度介绍中国国防费情况。白皮书梳理了改革开放以来中国国防费的发展历程，全面介绍 2012 年以来中国国防费的规模结构和基本用途，体现出中国国防费的公开透明。此外，白皮书还对国防费进行国际比较，说明中国国防开支是合理适度的。

第六，深入介绍中国军队维护世界和平稳定、服务构建人类命运共同体所做的积极努力和重大贡献。白皮书指出，构建人类命运共同体，顺应和平发展的时代潮流，反映各国人民共同期待。白皮书从维护联合国宪章宗旨和原则、推动构建新型安全伙伴关系、推动构建地

区安全合作架构、妥善处理领土问题和海洋划界争端、积极提供国际公共安全产品等 5 个方面进行了详细介绍。

新版白皮书在继承传统的基础上进行了创新发展，与过去相比主要有以下特点

第一，首次构建新时代中国防御性国防政策体系。白皮书阐明中国的社会主义国家性质、走和平发展道路的战略抉择、独立自主的和平外交政策、“和为贵”的中华文化传统，决定了中国始终不渝奉行防御性国防政策。白皮书通过丰富完善国防政策新的时代内涵，揭示了中国防御性国防政策的战略性、稳定性和系统性。

第二，首次阐述中国军队新时代的使命任务。白皮书明确阐述中国军队新时代的使命任务为“四个战略支撑”，即：为巩固中国共产党领导和社会主义制度提供战略支撑，为捍卫国家主权、统一、领土完整提供战略支撑，为维护国家海外利益提供战略支撑，为促进世界和平与发展提供战略支撑。白皮书通过介绍中国军队履行使命任务的具体实践，阐明武装力量建设运用的防御性、正义性、有限性。

第三，首次指出“永不称霸、永不扩张、永不谋求势力范围”是新时代中国国防的鲜明特征。白皮书重申我国国防自卫防御的本质属性，强调中国的国防建设和发展，始终着眼于满足自身安全的正当需要，始终是世界和平力量的增长。白皮书通过政策宣示深刻揭示，中国决不走追逐霸权、“国强必霸”的老路，无论将来发展到哪一步，中国都不会威胁谁，都不会谋求建立势力范围。

第四，首次提出服务构建人类命运共同体是新时代中国国防的世界意义。白皮书深刻揭示中国梦与世界梦、中国国防和军队建设同世界和平稳定的内在必然联系，强调中国军队的发展壮大不仅为中国梦提供战略支撑，同时也是世界和平稳定的强大正能量。

第五，首次全景式展现中国深化国防和军队改革取得的历史性成就。白皮书系统呈现中国军队进入新时代以来，深入贯彻习近平强军思想、坚持走中国特色强军之路、全面深化国防和军队改革的情况，通过公布改革的时间表、路线图、“成绩单”，深刻揭示中国军队迈出构建中国特色军事力量体系的历史性步伐，展现人民军队新的体制、结构、格局和面貌。

第六，首次将国防费位居世界前列的国家进行国际比较。白皮书从国防费占国内生产总值比重、国防费占财政支出比重和人均国防费水平等三个维度，比较 2017 年国防费位居世界前列的国家有关情况，有力说明中国国防费增长是合理适度的，开支水平是偏低的。白皮书强调，中国国防开支与维护国家主权、安全、发展利益的保障需求相比，与履行大国国际责任义务的保障需求相比，与自身建设发展的保障需求相比，还有较大差距，将继续保持适度稳定增长。

白皮书中、英文版单行本已分别由人民出版社、外文出版社出版，即日起在全国新华书店发行。（来源：共青团中央）

➢ 促进数据有序开发和共享

我们已经进入移动互联网、大数据时代，大数据的开发和共享成为一个蓬勃兴起的产业。大数据能够记录过去发生的事情，分析人们现在的行为状态，并预测人们未来的活动轨迹。数据的开发和共享也成为信息利用的一种重要方式，对经济运行、生活方式、社会治理产生重要影响。

与个人相关的数据往往包含大量个人信息和隐私，甚至涉及个人的敏感信息和核心隐私，一些机构也可以从数据中分析出个人的身份、财产、消费习惯等。因此，数据开发和共享与个人信息、隐私保护的关系十分密切。数据开发和共享的过程既涉及数据的流转，也涉及个人信息的收集、利用。同时，个人信息还可以通过共享被多次加工、利用。如果不加以规范，一旦数据共享行为失控，就可能导致大量个人信息被严重泄露或不当使用。因此，有必要对数据开发和共享行为设置专门规范，加强对个人信息和隐私等权利的保护，促进数据产业健康发展。

应在坚持保护个人基本信息权利的前提下，促进数据开发和共享。网络安全法第四十一条规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经信息被收集者同意。知情同意是

信息权利人对其个人信息支配权的具体体现，这种支配应当是一种独占性的支配。这种支配的效力不仅体现在个人信息的初次收集方面，也应当体现在数据开发和共享行为中。也就是说，信息收集者在初次收集个人信息时，原则上应当征得个人的同意；其在共享所收集到的个人信息时，同样应当取得个人的同意。这是因为，信息权利人允许信息收集并不等于允许信息共享。

因此，数据开发后再次共享的，如果涉及个人信息，应当获得信息权利人的明确授权。也就是说，信息无论与谁共享，在共享的范围内，都应当经过信息权利人的知情同意。除信息权利人对信息共享者有特别授权外，信息共享者对相关信息所享有的权利不得超出被明确授予的权利范围。如果信息权利人没有对共享后的信息使用作出单独授权，那么，信息共享者所获得的利用信息的权利不得超出信息权利人初次授权的范围。这实际上体现了对信息权利人控制其个人信息流通权利的尊重。

数据开发和共享中收集、使用个人信息，除了应当遵循合法、正当、必要的原则，还应当遵循最小化使用原则。这就是说，从事某一特定活动，在可以使用、也可以不使用个人信息时，尽量不使用；在必须使用并征得信息权利人许可时，尽量少使用。

在我国大数据产业发展过程中，既要鼓励数据开发、利用和共享，以充分发挥信息的效用，也要注重保护信息权利人的个人信息和隐私等权利。既不能因为过度保护个人信息权利而限制数据产业发展，也不能为发展数据产业而不考虑个人信息权利保护。企业在进行数据开发和共享时，应对相关数据是否涉及个人信息、隐私进行必要审查，遵循法律保护个人信息、隐私的一般规则。可以探索建立明确的数据保密等级与公开等级，既充分保障个人隐私、个人信息等权利，也为数据的利用、流通等提供便利，以促进数据有序开发和共享。（来源：人民日报 作者为中国人民大学常务副校长、法学院教授）

➢ 《信息安全技术网络安全等级保护测评要求》GB/T28448-2019 标准解读

引言：信息系统等级保护系列国家标准在我国推行信息安全工作开展过程中发挥了重要作用，被广泛应用于网络安全职能部门、各行业和领域的网络安全管理部门及等级测评机构开展系统定级、安全建设整改、等级测评、安全自查和安全监督检查等相关工作。但随着 IT 技术的飞速发展，特别是在云计算、移动互联、物联网、工业控制和大数据等新技术、新应用环境下，GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求》和 GB/T28448-

2012《信息安全技术信息系统安全等级保护测评要求》在应用过程中遇到了一些新的问题，在适用性、时效性、易用性、可操作性上需要进一步完善。

2017 年 6 月 1 日颁布实施的《中华人民共和国网络安全法》也要求各网络安全职能部门、各行业和领域的网络安全管理部门等配合落实国家网络安全等级保护制度，需要同时对 GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求》和 GB/T28448-2012《信息安全技术信息系统安全等级保护测评要求》进行修订。为适应我国网络安全等级保护工作发展的需要，进一步与新版的 GB/T22239-2019 相协调，有必要对 GB/T28448-2012 进行修订。

2014 年，公安部第三研究所（公安部信息安全等级保护评估中心）根据国家标准编号制修订计划，牵头组织了对 GB/T28448-2012 的修订工作，前后共有 20 多家单位、70 多人参与修订工作。修订工作历经调查研究、草案形成、征求意见稿、送审稿和报批稿等过程[8，9]，收到了各行业职能部门、用户、专家的宝贵意见。2019 年，《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）国家标准正式实施。本文分析了 GB/T28448-2019 发生的主要变化，解读其内容修订和等级测评工作变化等主要内容，以便读者更好地了解和掌握 GB/T28448-2019 的内容。

一、标准主要内容变化

1.1 标准文本结构变化

GB/T28448-2019 标准文本分为 12 章，3 个附录。第 1 章、第 2 章、第 3 章为标准的常规性描述，包括范围、规范性引用文件、术语和定义;第 4 章为缩略语;第 5 章概要描述了安全等级保护测评方法及单项测评和整体测评的构成。

第 6 章、第 7 章、第 8 章、第 9 章为重点章节，分别描述了第一级、第二级、第三级、第四级测评要求，以及每级如何遵从 GB/T22239-2019 的框架描述实施测评工作。每个级别都由五部分内容组成，包括安全通用要求、云计算、移动互联、物联网和工业控制系统等相关测评实施内容。安全技术方面从安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心 5 个方面展开;安全管理方面从安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理 5 个方面展开，与《基本要求》形成了相互对照、和谐统一的标准文本结构。

第 10 章为略掉的第五级测评要求。第 11 章描述了系统整体测评方法，在单项测评的基础上，从系统整体的角度综合考虑如何进行系统性的测评。分别从安全控制点测评、安全控制点间测评和区域间测评（包含层面间测评）等 3 个方面进行描述，分析了在进行系统整体测评时需要考虑的内容。第 12 章概要说明了测评结论的得出方法及测评结论主要包括的内容等。

表 1 不同级别的等级保护对象的测评力度要求

测评力度	测评方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

测评的广度和深度落实到访谈、核查和测试 3 种不同的测评方法上，能够体现出测评实施过程中访谈、核查和测试的投入程度的不同。**对于不同等级的测评工作的强度可由以下 3 个方面来体现：**

1）使用不同测评方法

在实际现场测评实施过程中，安全技术方面的测评方法以配置核查和测试验证为主。安全管理方面可以使用访谈方式进行测评。使用不同测评方法能体现出测评实施过程中访谈、核查和测试的测评强度的不同。

2）不同级别测评对象范围不同

第一级和第二级测评对象的范围为关键设备，第三级为主要设备，第四级为所有设备。不同级别测评对象范围不同，能体现出测评实施过程中访谈、核查和测试的测评广度的不同。

3）不同级别现场测评实施工作不同

第一级和二级以核查安全机制为主，第三级和第四级先核查安全机制，再测试验证安全策略的有效性。

二、新标准下的等级测评

2.1 标准使用

在针对某级别等级保护对象进行等级测评时，无论该等级保护对象使用何种特定技术或处于何种特定的应用场景，都必须使用安全测评通用要求对等级保护对象进行测评，再结合等级保护对象采用的具体技术架构或应用场景选用相关安全测评扩展要求进行等级测评。例如，某单位的等级保护对象采用了云计算技术和大数据技术，在进行等级测评时，首先使用 GB/T28448 中的安全测评通用要求部分，再使用大数据安全测评扩展要求部分和云计算安全测评扩展要求部分进行等级测评。

2.2 测评对象选择

由于新技术新应用的迅速发展，等级保护对象的形态发生了变化，导致等级测评对象也发生了变化。以云计算平台和传统信息系统的测评对象为例，测评对象选择如表 2 所示。

表 2 测评对象选择

安全类或层面	云计算平台测评对象	传统测评对象
安全物理环境	机房及基础设施	机房及基础设施
安全通信网络	网络结构、通信传输设备、可信验证设备、虚拟化网络结构	传统网络设备、传统安全设备、传统网络结构
安全区域边界	网络设备、安全设备、虚拟网络设备、虚拟安全设备	传统网络设备、传统安全设备、传统网络结构
安全计算环境	网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、数据库管理系统、终端、应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	传统主机、数据库管理系统、终端、应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

由表 2 可以看出，与传统信息系统相比，采用新技术新应用的等级保护对象的测评对象发生了很大变化。在进行等级测评时，应根据被测等级保护对象采用新技术新应用的情况，依据测评对象选择规则合理选择测评对象。

2.3 测评作业指导书开发

测评作业指导书的开发包括安全物理环境（包括相应的安全扩展要求）、安全通信网络（包括相应的安全扩展要求）、安全区域边界（包括相应的安全扩展要求）、安全计算环境（包括相应的安全扩展要求）、安全管理中心（包括云计算安全扩展要求）和安全管理（包括相应的安全扩展要求）等方面，其中，安全物理环境、安全通信网络、安全区域边界、安全管理中心和安全管理等为全局性测评，安全计算环境需要根据设备类型和型号分别制定作业指导书。

以云计算平台的安全区域边界和安全计算环境为例，安全区域边界属于全局性测评，此部分测评作业指导书的指标项和测评实施项来源于安全测评通用要求和云计算安全测评扩展要求中的相关部分。由于安全计算环境部分的测评作业指导书与设备类型和型号相关，所以可能涉及的作业指导书包括路由器（包括虚拟路由器）安全测评作业指导书、交换机（包括虚拟交换机）安全测评作业指导书、防火墙（包括虚拟防火墙）安全测评作业指导书、操作系统（包括虚拟机）安全测评作业指导书、数据库安全测评作业指导书、宿主机操作系统安全测评作业指导书和云操作系统安全测评作业指导书等。

2.4 单项测评

单项测评从安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心十个方面逐一展开。

1）安全物理环境单项测评

安全物理环境的单项测评主要针对机房的基础物理设施环境及相关的硬件设备和介质等进行。部分安全物理环境安全的测评涉及终端所在的办公场地。测评的主要内容包括物理位置选择、物理访问控制、防雷、防火、防水、防潮、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等。测评对象包括各种制度类、规程类、记录和证据类等文档，各类安全管理人员和机房各类基础设备。其中，各类安全管理人员主要为安全主管、系统管理员、审计管理员、安全管理员和其他相关人员;机房各类基础设备包括电子门禁系统、机房监控系统、防盗报警系统、防感应雷措施、火灾自动检测、报警和灭火、温湿度自动调控、UPS、备用发电系统和屏蔽机柜/机房等。

2）安全通信网络单项测评

安全通信网络的单项测评主要针对组织中的数据通信网络进行，由网络设备、安全设备和通信链路及其组件构成，目的是保证等级保护对象各个部分进行安全通信传输。测评内容主要包括网络架构、通信传输和可信验证等。测评对象包括路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，综合网管系统和相应设计/验收文档等。

3）安全区域边界单项测评

安全区域边界的单项测评主要针对系统边界进行，系统边界一般包括整网互联边界和不同级别系统之间的边界。测评内容主要包括边界防护、访问控制、入侵防范、恶意代码、反垃圾邮件防范和安全审计等。测评对象包括网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件，抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件，防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件，防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件，终端管理系统或相关设备等。

4）安全计算环境单项测评

安全计算环境的单项测评主要针对构成等级保护对象的所有设备节点进行。测评内容主要包括身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等。测评对象包括终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等、提供可信验证的设备或组件和提供集中审计功能的系统等。

5）安全管理中心单项测评

安全管理中心的单项测评主要针对相关的集中安全管理系统进行。测评内容主要包括系统管理、审计管理、安全管理和集中管控等。测评对象主要包括提供集中系统管理功能的系统、安全审计系统等提供集中审计功能的系统和综合网管系统等提供运行状态监测功能的系统等。

6）安全管理方面的单项测评

安全管理方面的单项测评主要包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维 5 个方面。测评对象主要包括人员和文档。人员包括系统管理员、

安全审计员、安全管理员、机房管理员和文档管理员等。文档包括管理文档（策略、制度、规程），记录类文档（会议记录、运维记录）和其他类文档（机房验收证明等）。

2.5 整体测评

等级保护对象整体测评需要从安全控制点测评、安全控制点间测评和区域间测评等方面进行综合安全分析，从而给出等级测评结论。

1）安全控制点测评

安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。在单项测评完成后，如果该安全控制点下的所有要求项为符合，则该安全控制点符合;否则，为不符合或部分符合。

2）安全控制点间测评

安全控制点间测评的目的是确定安全问题之间的关联对定级对象整体安全保护能力的影响，所以需要从同一安全类或层面内的两个或两个以上不同安全控制点间的测评结果进行关联综合分析。在单项测评工作完成后应进行安全控制点间测评，汇总统计定级对象的某个安全控制点中的要求项存在不符合或部分符合的情况，综合分析在同一安全类或层面内是否存在不同安全控制点之间具有增强或削弱的作用（如物理访问控制和防盗窃、身份鉴别和访问控制等）。同时分析是否存在与该要求项具有相似的安全功能的安全技术措施或管理措施等相关工作。

根据安全控制点间测评结果，综合分析判断其相对应的安全保护能力是否缺失，如果经过综合分析其相关联的安全问题不会造成定级对象整体安全保护能力的缺失，则该安全控制点测评结果应调整为符合。

3）区域间测评

区域间测评的目的是确定安全问题之间的关联对定级对象整体安全保护能力的影响，所以需要从不同功能区域间或不同控制方式之间的关联进行测评分析。在单项测评工作完成后应进行区域间测评，汇总统计定级对象的某个安全控制点下的安全要求项不符合或部分符合的情况。分析在互连互通的不同安全区域之间，是否存在区域间安全功能的相互增强或削弱等作用，重点分析定级对象的访问控制路径，如不同功能区域间的数据流流向和控制方式。

根据区域间测评结果，综合分析判断与其相对应的安全保护能力是否缺失，如果经过综合分析其相关联的安全问题不会造成定级对象整体安全保护能力的缺失，则该安全控制点测评结果应调整为符合。

2.6 测评结论形成

等级测评结论的形成需要分析汇总单项测评结果中存在的不符合项或部分符合项，采用风险分析方法对所有安全问题进行风险评价，通过整体测评再对安全问题进行关联分析，分析安全问题被威胁利用的可能性，判断其被威胁利用后对业务系统安全造成的影响程度。综合评价这些安全问题对定级对象造成的安全风险，并给出等级保护对象的等级测评结论。等级测评结论包括符合、基本符合和不符合 3 类，具体描述如下：

1）符合

定级对象未发现安全问题，单项测评结果中部分符合和不符合项的统计结果全为 0，综合得分为 100 分。

2）基本符合

定级对象存在安全问题，部分符合和不符合项的统计结果不全为 0，但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于阈值。

3）不符合

定级对象存在安全问题，部分符合项和不符合项的统计结果不全为 0，且存在的安全问题会导致定级对象面临高等级安全风险，或者综合得分低于阈值。

三、结束语

GB/T28448-2019 已经正式发布实施，与 GB/T28448-2012 相比，其标准文本结构和内容都发生了很大变化，对安全测评服务机构、等级保护对象的运营使用单位及主管部门的等级保护推进工作产生较大影响。本文通过深入分析新标准 GB/T28448-2019 的主要变化，着重介绍了如何基于新标准开展等级测评工作，从而帮助安全测评服务机构、等级保护对象的运营使用单位及主管部门更好地了解和掌握新标准的主要内容，同时也为网络安全职能部门开展执法检查提供参考。（来源：公安部信息安全等级保护评中心 陈广勇）

➢ 未成年人网络保护将有法可依

近日，共青团中央召开 2019 年办理全国人大代表建议、全国政协委员提案座谈会。据相关媒体报道，今年拟提请全国人大常委会会议审议的未成年人保护法修订草案，将增设网络保护的章节。与此同时，酝酿多年的《未成年人网络保护条例》，今年有望出台。这无疑向广大公众释放出一个重要信号：未成年人网络保护将有法可依。

沉迷网络引发问题多

未成年人网络保护向来是家长、政府及社会密切关注的问题。随着互联网渗透人们生活的方方面面，互联网的普及率也大大增加。第 43 次《中国互联网络发展状况统计报告》显示，截至 2018 年 12 月，中国网民规模为 8.29 亿，普及率达 59.6%。这其中，19 岁以下网民占 21.6%，人数超过 1.79 亿。另据数据显示，未成年人 10 岁之前触网比例高达 72%，首次触网年龄持续走低。

作为互联网的原住民，“00 后”自诞生起就与互联网相伴成长。该群体对于互联网的熟悉程度远超过其他年龄群体，思维方式和行为方式也深受网络影响。利用互联网学习知识、开阔眼界，一方面，网络丰富了未成年人的成长生活；另一方面，由于未成年人心智发展尚未成熟，很容易受暴力、血腥、色情等不良网络内容的影响。

在青少年网民群体急剧增加的同时，未成年人因沉迷网络造成不良后果的新闻也屡见报端。“10 岁小学生偷刷父亲银行卡充值网游”“16 岁少年偷钱打赏女主播 40 万元”……因青少年沉迷网络导致的诸多问题困扰着许多家庭，也逐渐演变为严重的社会问题。2018 年 9 月，国家卫健委举行的新闻发布会对外公布，全球青少年过度依赖互联网的比例为 6%，中国接近 10%。同年，世界卫生组织将网络成瘾障碍纳入精神心理疾病的一类。

沉迷网络不仅影响未成年人的心理健康，更对未成年人的身体健康产生影响。数据显示，2018 年，中国小学生近视比例已达 45.7%，初中生近视比例为 74.4%，高中生近视比例为 83.3%。除了先天性因素之外，网络设备使用频率的增加，对加深青少年近视起了负面作用。

现行法律监管不足

针对这些现象，社会各界对防止未成年人沉迷网络、加强未成年人网络保护的呼声日益增强。在今年的全国两会上，马化腾、丁磊等互联网行业代表均就加强未成年人网络保护、打造安全健康的青少年网络生态进行了发言。

目前，中国规范网络游戏的具体规定包括原文化部颁布的《网络游戏管理暂行办法》和《关于严格规范网络游戏市场管理的意见》，立法领域尚属空白。关于未成年人网络保护，中国在《未成年人保护法》和《网络安全法》中做了相关的原则性规定。然而，随着网络对人们生活的不断渗透和未成年人网络沉迷现象的复杂化，现行管理办法的针对性、操作性有限，越来越不能满足当前未成年人网络保护的需要。有专家认为，目前包括防沉迷在内的涉及网络游戏内容等方面的规定都过于笼统，并没有可以具体可执行的、操作性强的条款。

什么是防沉迷系统？平台运用何种技术防沉迷？技术标准是什么？筛选适合青少年查看的网络内容标准是什么？目前，这些问题往往缺乏明确统一的规定，大多根据企业内部标准，这也使不同企业在防沉迷系统的设置上松严不一。中国政法大学传播法研究中心副主任朱巍认为：“最重要的是建立统一的标准。有些游戏公司严格实行了实名制，有些却没有，不能让‘劣币驱逐良币’。”缺乏具体的法律标准，也使许多推进未成年人法律保护的措施难以落地。

将未成年保护落到实处

尽管目前中国在未成年人网络保护的立法方面还存在空缺，不过这次提案座谈会公布的信息，将使这一问题有望得到解决。专家认为，加快未成年人网络保护的立法工作，回应了社会密切关注的问题，有利于从源头和机制上保护未成年人合法权益、促进未成年人的健康成长。

将网络保护章节写入《未成年人保护法》修订草案、出台《未成年人网络保护条例》，通过立法建立行为准则、约束准则，在有法可依的基础上，专家建议，相关职能部门、网络平台和家长学校都应承担起责任。未成年人网络保护，向来都不是单方的责任。

首先，职能部门应明确监管职责，依法严格监督和审核相关网络平台开发商及运营商对制度的落实情况，对于违规行为要加强惩处力度；立法部门也需要通过不断细化法律法规以应对新的情况。其次，相关网络企业应积极承担企业责任，保护用户尤其未成年人的个人信息和隐私，落实好防沉迷系统和网络实名制，对用户作出成年和未成年之分，从而对使用时间和内容作出区分。最后，还要建立家校合作协作机制，第一时间对沉迷网络的学生加以心理分析和疏导，配合监护人开展家庭教育。同时，也应倾听未成年人的心声和意见。如此才能更好地将未成年人网络保护落到实处。（来源：人民日报-海外版）

四、政府之声

➢ 国家网信办等 4 部门发布《云计算服务安全评估办法》附解答

2019 年 7 月 22 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部关于发布《云计算服务安全评估办法》的公告 2019 年第 2 号：为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部制定了《云计算服务安全评估办法》，现予以发布。

《云计算服务安全评估办法》有关问题解答如下：

1、组织开展云计算服务安全评估的目的是什么？

答：开展云计算服务安全评估，是为了提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，降低采购使用云计算服务带来的网络安全风险，增强党政机关、关键信息基础设施运营者将业务及数据向云服务平台迁移的信心。

2、云计算服务安全评估的对象是什么？

答：云计算服务安全评估是依据云服务商申请，对面向党政机关、关键信息基础设施提供云计算服务的云平台进行的安全评估。同一云服务商运营的不同云平台，需要分别申请安全评估。

3、何时起云服务商可申请评估？需要提交哪些材料？

答：自 2019 年 9 月 1 日起云服务商可以正式提交云计算服务安全评估申请。需要提交

的材料包括申报书、云计算服务系统安全计划、业务连续性和供应链安全报告、客户数据可迁移性分析报告等。有关申报材料模版将在中国网信网提供下载。

4、已通过党政部门云计算服务网络安全审查的云平台，是否还需要申请云计算服务安全评估？

答：前期已经通过党政部门云计算服务网络安全审查的云平台，视同为已通过云计算服务安全评估，不需要再重新申请。

5、云计算服务安全评估主要参照哪些标准？

答：云计算服务安全评估主要参照国家标准《云计算服务安全能力要求》、《云计算服务安全指南》，其中《云计算服务安全能力要求》从系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境安全等方面提出要求。

6、云计算服务安全评估有哪些主要环节？

答：主要包括申报、受理、专业技术机构评价、云计算服务安全评估专家组综合评价、云计算服务安全评估工作协调机制审议、国家互联网信息办公室核准、评估结果发布、持续监督等环节。

7、云计算服务安全评估结果在哪里查询？有效期多长时间？

答：评估结果将由国家互联网信息办公室网络安全协调局在中国网信网公布。评估结果有效期为 3 年。

8、云计算服务安全评估如何保护被评估方的商业秘密和知识产权？

答：云计算服务安全评估过程中，参与评估工作的单位和人员对云服务商提交的非公开材料或在评估中获悉的非公开信息承担保密义务，严格保护云服务商的商业秘密和知识产权。如果云服务商认为有关单位和人员未能承担保密义务的，可以向国家互联网信息办公室或有关部门举报。

9、关于云计算服务安全评估问题可向谁咨询？

答：有关云计算服务安全评估的其他具体事项，可发送电子邮件到 yunpinggu@cac.gov.cn 或拨打 010-55635861 咨询。（来源：国家互联网信息办公室）

- **《云计算服务安全评估办法》的公告**
- **全文：**http://www.cac.gov.cn/2019-07/22/c_1124781475.htm

➢ 互联网信息服务严重失信主体信用信息管理办法（征求意见稿）发布

2019 年 7 月 22 日，国家互联网信息办公室就《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》公开征求意见。根据征求意见稿，对纳入失信黑名单的互联网信息服务提供者和使用者将依法依规实施限制从事互联网信息服务、网上行为限制、行业禁入等惩戒措施。

征求意见稿提出，网信部门会同有关部门对互联网信息服务严重失信主体实施信用黑名单管理和失信联合惩戒，适用该办法。互联网信息服务严重失信主体，是指在中华人民共和国境内提供、使用互联网信息服务中存在严重失信行为的相关主体。

根据征求意见稿，互联网信息服务提供者和使用者有因违反互联网信息内容管理相关法律法规，被网信部门单独或会同有关部门处以关闭网站、吊销相关业务许可证或者吊销营业执照、撤销许可或者取消备案的行政处罚；通过网络编造、发布、传播违背社会公德、商业道德、诚实信用等信息，或者故意为编造、发布、传播违背社会公德、商业道德、诚实信用等信息提供技术、设备支持或者其他服务，严重破坏网络空间传播秩序，损害社会公共利益和人民群众合法权益，造成恶劣社会影响；违反法律、行政法规规定，失信情节严重等情形之一的，网信部门认定为互联网信息服务领域严重失信行为，行为主体列入互联网信息服务

严重失信主体黑名单。对在互联网信息服务领域发生较重失信行为或多次发生轻微失信行为但尚未达到黑名单认定标准的相关失信主体，列入重点关注名单。

征求意见稿明确，黑名单有效期一般为 3 年，黑名单信息发布时限与其有效期一致。此外，黑名单主体通过主动纠正失信行为、消除不良社会影响等方式修复信用，并按照社会信用体系建设有关规定履行相关义务，向认定部门申请退出黑名单的，经认定部门同意，可提前退出黑名单。（来源：国家互联网信息办公室）

- **《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-07/22/c_1124782573.htm

➢ 工信部召开 2019 年网上“扫黄打非”工作部署电视电话会议

2019 年 7 月 25 日，工业和信息化部信息通信管理局组织召开 2019 年网上“扫黄打非”工作部署电视电话会议。工业和信息化部信息通信管理局副局长鲁春丛、中共中央宣传部反非法反违禁局(全国“扫黄打非”办公室)副局长许文彤出席会议并讲话。工业和信息化部相关司局，各省(自治区、直辖市)通信管理局，中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国互联网协会，基础电信企业、网络接入服务企业相关负责人出席会议。

会议指出，网上“扫黄打非”工作是网络安全工作的重要组成部分，今年将继续强化互联网基础管理，细化工作措施，创新技术手段，加大监管力度，压实企业主体责任，严厉打击网络违法违规行为，净化网络空间，切实维护人民群众利益。

会议强调，信息通信行业要以习近平新时代中国特色社会主义思想为指导，全力以赴做好网上“扫黄打非”工作，为庆祝新中国成立 70 周年营造健康清朗的网络环境。（来源：工业和信息化部）

➢ 上海召开 2019 年关键信息基础设施网络安全检查动员部署会

2019 年 7 月 25 日下午，为深入贯彻落实习近平总书记关于加强关键信息基础设施网络安全保护的重要指示，落实《网络安全法》相关规定，切实压实网络安全责任，提升安全防护水平，2019 年上海市关键信息基础设施网络安全检查动员部署会在市委党校召开。市委常委、宣传部部长周慧琳出席会议并讲话。

会议要求，各单位要充分认识关键信息基础设施保护对于城市发展的重要性，坚决贯彻中央和市委的工作部署，切实抓好关键信息基础设施网络安全工作。要坚持问题导向，深入排查突出问题和风险隐患，采取切实措施，全面提升关键信息基础设施网络安全防护能力。

会议强调，做好今年关键信息基础设施网络安全检查工作，重在“四个加强”。一是加强工作统筹协调，形成密切配合、高效处置的“大网信”格局;二是加强关键领域排查，安全检查要不留空白，更要抓住重点、抓住关键;三是加强主体责任落实，行业主管部门和各区委网信办要履行好指导和监管责任，各设施运营者要切实承担起主体责任;四是加强问题整改落实，市委网信办和各行业主管部门要加强整改落实的督导，对拒不整改或整改不力的单位要严肃约谈。

本次检查时间为 7 月至 9 月，共分为部署、培训、自查、抽查和总结五个阶段。各区、各行业主管部门将组织本区、本行业关键信息基础设施运营单位开展自查和整改工作，检查工作领导小组办公室将组织抽查和督导工作，汇总上报数据，总结评估检查情况。（来源：网信上海）

五、本期重要漏洞实例

➢ Adobe Experience Manager 跨站请求伪造漏洞

发布日期：2019-08-01
更新日期：2019-08-01
受影响系统：
Adobe Experience Manager 6.4
Adobe Experience Manager 6.3
Adobe Experience Manager 6.2
Adobe Experience Manager 6.1
Adobe Experience Manager 6.0
不受影响系统：
Adobe Experience Manager 6.4.5.0
描述：

BUGTRAQ ID: 109129
CVE(CAN) ID: CVE-2019-7953
Adobe Experience Manager 是美国 Adobe 公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案，支持移动内容管理、营销销售活动管理和多站点管理等。
Adobe Experience Manager 6.4 及之前版本中存在跨站请求伪造漏洞，该漏洞源于未合理验证 HTTP 请求。攻击者可利用该漏洞导致当前用户上下文中的敏感信息泄露。
<*来源：Adobe
链接：https://helpx.adobe.com/security/products/experience-manager/apsb19-38.html
*>
建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB19-38）以及相应补丁：
APSB19-38：Security updates available for Adobe Experience Manager
链接：https://helpx.adobe.com/security/products/experience-manager/apsb19-38.html

➢ 多个卡巴斯基产品信息泄露漏洞

发布日期：2019-08-01
更新日期：2019-08-01
受影响系统：
Kaspersky Labs Kaspersky Antivirus 2019

Kaspersky Labs Kaspersky Internet Security 2019
Kaspersky Labs Kaspersky Total Security 2019
不受影响系统：
Kaspersky Labs Kaspersky Antivirus 2019 Patch F
Kaspersky Labs Kaspersky Internet Security 2019 Patch F
Kaspersky Labs Kaspersky Total Security 2019 Patch F
描述：

BUGTRAQ ID: 109300
CVE(CAN) ID: CVE-2019-8286
Kaspersky Anti-Virus 等都是俄罗斯 Kaspersky 实验室开发的一套杀毒软件。Kaspersky Internet Security 是一套同时具有反病毒和防火墙功能的安全软件。Kaspersky Total Security 是一套全功能安全软件。
Kaspersky Anti-Virus、Kaspersky Internet Security、Kaspersky Total Security 2019 及之前版本中存在信息泄露漏洞。攻击者可利用该漏洞强迫受害者访问特制的页面（如通过点击网络钓鱼链接）泄露唯一的产品 ID。

<*来源：Ronald Eikenberg
链接：https://support.kaspersky.com/general/vulnerability.aspx?el=12430#080719
*>

建议：

厂商补丁：
Kaspersky Labs

Kaspersky Labs 已经为此发布了一个安全公告（CVE-2019-8286）以及相应补丁：
CVE-2019-8286：Kaspersky Advisory issued on 11th July, 2019
链接：https://support.kaspersky.com/general/vulnerability.aspx?el=12430#080719

➢ Mozilla Firefox 多个未明内存损坏漏洞

发布日期：2019-07-30
更新日期：2019-07-31
受影响系统：
Mozilla Firefox 67
描述：

BUGTRAQ ID: 109081
CVE(CAN) ID: CVE-2019-11710
Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。
Mozilla Firefox 67 版本中存在多个未明内存损坏漏洞.攻击者可利用该漏洞在受影响应用程序的上下文中执行任意代码。

<*来源：AndréBargull，Christian Holler，Natalia Csoregi，Raul Gurzau，Daniel Varga，Jon Coppeard，Marcia Kn
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/
*>
建议：

厂商补丁：
Mozilla

Mozilla 已经为此发布了一个安全公告（CVE-2019-11710）以及相应补丁：
CVE-2019-11710：Mozilla Foundation Security Advisory 2019-21
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/

➢ IBM Jazz for Service Management 信息泄露漏洞

发布日期：2019-07-30
更新日期：2019-07-30
受影响系统：
IBM Jazz for Service Management 1.1.3.2
IBM Jazz for Service Management 1.1.3
描述：

BUGTRAQ ID: 109144
CVE(CAN) ID: CVE-2019-4193
IBM Jazz for Service Management 是美国 IBM 公司的一款提供对服务管理环境可见性的集成服务管理产品。
IBM Jazz for Service Management 1.1.3 和 1.1.3.2 版本中存在信息泄露漏洞，该漏洞源于将敏感信息存储在 URL 参数中。未授权的攻击者可利用该漏洞通过服务器日志、referrer 报文头或浏览器历史记录获取 URL 访问权限导致信息泄露。
<*来源：IBM （ncsupp@ca.ibm.com）
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10885985
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（159032）以及相应补丁：
159032：Security Bulletin: IBM Jazz for Service Management stores sensitive information in URL parameters (CVE-2019-4193)
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10885985

六、本期网络安全事件

➢ 美国第一资本银行遭黑客入侵：逾 1 亿用户信息泄露

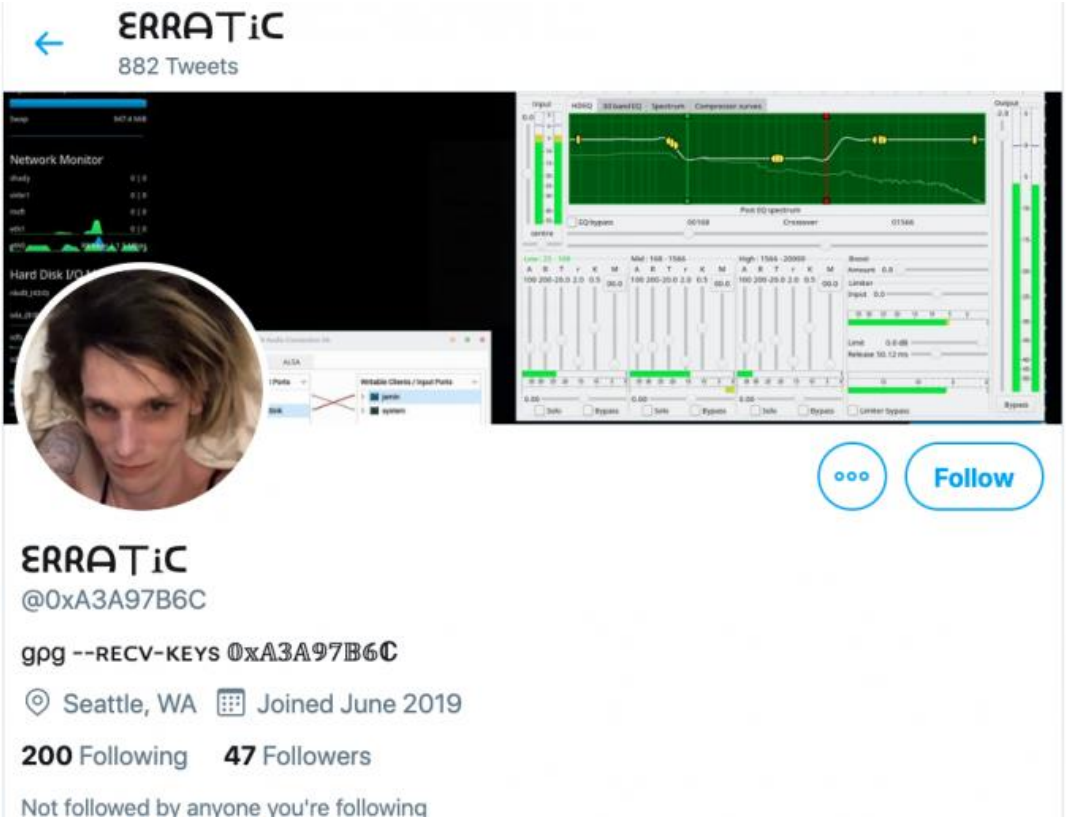
2019 年 7 月 30 日，美国第一资本银行金融公司在周一披露，一名黑客获取了逾 1 亿名顾客和潜在顾客的个人信息，包括姓名、地址、电话号码和生日。美国第一资本称，公司在 7 月 19 日确认了这次黑客入侵事件，目前这名黑客已经被美国联邦调查局逮捕。在宣布这一消息后，第一资本股价在盘后交易中下跌 1%。

美国第一资本表示，大约有 1 亿美国用户和 600 万加拿大用户的个人信息受到了此次事件的影响，但是黑客没有获取任何信用卡账号，超过 99%的社会安全号码没有泄露。根据美国第一资本披露的信息，包括 2005 年至 2019 年初信用卡申请者在内的基本个人信息被黑客访问，包括信用评分、支付历史以及部分交易数据。大约 14 万个美国顾客的社会安全号码以及 8 万个关联银行账号被获取。在加拿大，100 万个社保账号被黑客访问。

美国第一资本表示，将向受影响的个人通知这次入侵事件，并提供免费的信用监控和身份保护服务。

2019 年 7 月 31 日，33 岁前亚马逊 AWS 雇员 Paige A.Thompson(佩吉汤普森)周一遭到逮

捕，被控入侵第一资本的网络，窃取了用户的敏感数据。暴露的用户信息包括名字、收入、生日、地址、手机号码、电邮地址，14 万美国用户和 100 万加拿大用户的社会安全号码被盗，8 万银行账号被访问。



信用卡号码或登录凭证没有失窃。Thompson 被指利用第一资本网络防火墙的漏洞在其服务器上执行一系列命令，其中一个命令被用于获取管理员账号*****WAF-Role 的凭证。第一资本租赁了 AWS 的服务器，IP 地址和其它证据显示是 Thompson 利用了漏洞并将数据发布在其 Github 账号内。Thompson 尝试利用 IPredator 的 VPN 和 Tor 来隐藏入侵痕迹，但却在社交媒体上公开了许多入侵证据。

入侵发生在 3 月 22 日左右，但直到 7 月 17 日第一资本收到有人发出的邮件警告，报告 Thompson 的 Github 账号发布了敏感用户数据。2019 年 7 月 19 日第一资本证实了入侵。Thompson 的 Github 账号(镜像)包含了她的 LinkedIn 链接。

Paige A.Thompson(佩吉汤普森)对于自己的黑客工作，汤普森从不避讳，她还在网络上组织了一个 “对分布式系统、编程、黑客攻击和破解感兴趣”的小组。此次泄露事件后，她曾尝试在网上与人分享这些信息，甚至留下线索供警察调查。据悉，黑客攻击是从今年 3 月 12 日开始的，一直持续到 7 月 17 日。目前汤普森已因涉嫌计算机欺诈和滥用职权在西雅图被捕。

此次事件将为第一资本带来 1.5 亿美元的损失，将用于为受影响客户支付信贷监控费用、科技修复、法律维护等工作。Capital One 发布声明表示，此次事件没有信用卡帐号或登录凭据被泄露，超过 99%社会保障号未受损。同时银行已在第一时间修复了漏洞，并承诺将为受影响的每个人提供免费的信用监控和身份保护。

受此事件影响，第一资本金融(COF)最新一个交易日股价下跌 5.89%，报 91.21 美元。财报显示，第一资本 2018 财年年报归属于普通股东净利润为 57.10 亿美元，同比增长 235.09%；营业收入为 280.76 亿美元，同比上涨 3.08%。（来源：互联网综合整理）

➢ 做广告送小区业主信息，江苏南通 12 人侵犯公民个人信息获刑

2019 年 7 月 19 日，为了增加自己的销售业绩，江苏省南通市一家广告公司业务员在非法获取大量公民个人信息后，做起了“给我做广告，我就送你小区业主信息”的“生意”，结果连同他在内的 12 名被告人一同站上了法庭的被告席。7 月 16 日，江苏省南通市中级人民法院对此案作出维持一审的终审刑事裁定，被告人孔某以侵犯公民个人信息罪判处有期徒刑三年，并处罚金 5000 元；被告人张某等 9 名被告人宣判不等缓刑并分处罚金，被告人沈某、刘某被免予刑事处罚。

被告人孔某系南通一家广告公司负责小区广告推送的业务员，中专文化。在很多人看来，

广告业务员是一种入门低，而又能赚大钱的职业，但这个前提是必须经常接到业务。进入 2015 年下半年，孔某的广告销售业绩连续几个月在公司排名垫底，收入自然也一落千丈。此前，孔某曾在几家房地产公司做过销售，认识不少房地产公司做销售的“兄弟们”，为了增加自己的销售业绩，孔某萌生了做广告送小区业主信息的念头。

2015 年底，孔某向南通某房地产公司销售员沈某索要了南通某小区楼盘含有小区名称、楼幢号、单元号、楼层、业主姓名、联系方式等内容的公民个人信息共计 1729 条。被告人刘某系某品牌衣柜的加盟商，在一个微信群里看到孔某发布的做广告送小区业主信息的消息后，主动加了孔某的微信，在谈好让对方帮着在南通某小区投放衣柜广告，并支付相关费用后，孔某如约将上述 1729 条业主信息原封不动的发给了刘某。

2016 年 1 月至 4 月间，孔某又从好友高某（另案处理）处获取到南通市多家小区楼盘含有业主姓名、联系方式、房号等内容的公民个人信息 8594 条，其中 3000 余条涉及房屋面积信息，还有部分涉及到了车库号、车库面积、业主居民身份证号码、配偶和子女的姓名及联系方式等一种或多种信息。

后孔某在推销其广告业务的同时，将以上公民个人信息向张某等 10 人出售或免费提供，其中含有业主姓名、联系方式、房号等内容的公民个人信息累计达 10 万余条，非法获利 1200 元。案发后，12 名被告人在接到办案民警电话通知后均主动到案，并如实供述了自己的罪行。

南通经济技术开发区人民法院经审理认为，被告人孔某违反国家有关规定，以其他方法非法获取公民个人信息，向他人出售、提供公民个人信息，情节特别严重；被告人沈某向他人提供公民个人信息，情节严重；被告人张某等 9 名被告人非法获取公民个人信息，情节特别严重；被告人刘某非法获取公民个人信息，情节严重，上述 12 名被告人的行为均已构成侵犯公民个人信息罪。本案中，除孔某、沈某有提供或出售行为外，其余涉案 10 名被告人在实施犯罪行为时均有正当的工作，基本都以开展业务、提高业绩为初衷，最终实施了本案所涉的犯罪行为，现有证据证明涉案公民个人信息基本未用于进一步的传播、扩散，且至案发尚未造成引发其他犯罪等严重的实际危害后果，各被告人归案后认罪态度较好，对其均可酌情从轻处罚。

综合各被告人的犯罪事实、犯罪情节、认罪态度、悔罪表现及具备的监管条件等，法院遂作出上述判决。张某等部分被告人认为，案涉公民个人信息不属司法解释规定的“非法获取、出售或者提供住宿信息、通信信息、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息”，应认定为普通公民个人信息，达到 5000 条以上才能入罪。为此，

向二审法院提起上诉。南通中院经审理维持了原判。

■连线法官■：该案二审合议庭审判长杜开林介绍说，随着互联网技术的快速发展，公民个人信息被他人或单位肆意获取和利用的情形时有发生，公民个人信息安全也受到很大的威胁。《中华人民共和国刑法》第二百五十三条之一第二款规定，以窃取或者其他方法非法获取国家机关或者金融、电信、交通、教育、医疗等单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的行为，可处三年以下有期徒刑或者拘役，并处或者单处罚金。

杜开林介绍说，为了依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，从 2017 年 6 月 1 日起施行的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第四条规定，违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。同时第五条第四款规定，非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的，应当认定为刑法第二百五十三条之一规定的“情节严重”。

本案中，经查，案涉公民个人信息系以小区、楼盘业主信息为主，主要包含房号、业主姓名、电话号码、家庭住址等，有多家楼盘还涉及房屋面积、拆迁房屋面面积、安置面积等信息，该信息与“住宿信息、通信信息、健康生理信息、交易信息”具有同等重要性，应认定司法解释所规定的“其他可能影响人身、财产安全的公民个人信息”，且数量达到司法解释所规定的情节严重、情节特别严重标准的 500 条、5000 条以上。故依法均应以侵犯公民个人信息罪追究各涉案人员的刑事责任。（来源：中国法院网）

➢ 美国路易斯安那多学区遭网络攻击 宣布进入紧急状态

2019 年 7 月 27 日，近年来美国地方政府不断受到勒索软件和网络攻击的威胁。继 2018 年 2 月受到 SamSam 勒索软件攻击，导致科罗拉多州交通局被迫关闭运营之后，最近路易斯安那州州长乔恩·贝尔·爱德华兹宣布该州的多个学区遭受了严重的网络攻击，并宣布该州进入紧急状态。

据报道，路易斯安那州北部的三个教区（Sabine，Morehouse 和 Ouachita）遭到袭击，这些袭击事件摧毁了 IT 网络并加密了文件，使其无法访问。目前该地区已经启动了紧急预案，在联邦执法部门提供的帮相下，路易斯安那国民警卫队报告称已派出一个网络团队帮助恢复当地系统并安装防火墙。

这些受影响学区在其官方网站上发布了一则声明，表示 Sabine 教区学校系统在星期天早上遭到电子病毒攻击。声明中写道：“这种病毒已经禁用了我们的一些技术系统和我们的中心办公电话系统。该地区的工作人员向当地执法部门，州官员和联邦调查局报告了这起电子病毒袭击。正在利用所有可用资源使区域系统重新恢复上线。目前正在进行配合地方，州和联邦执法的调查。”

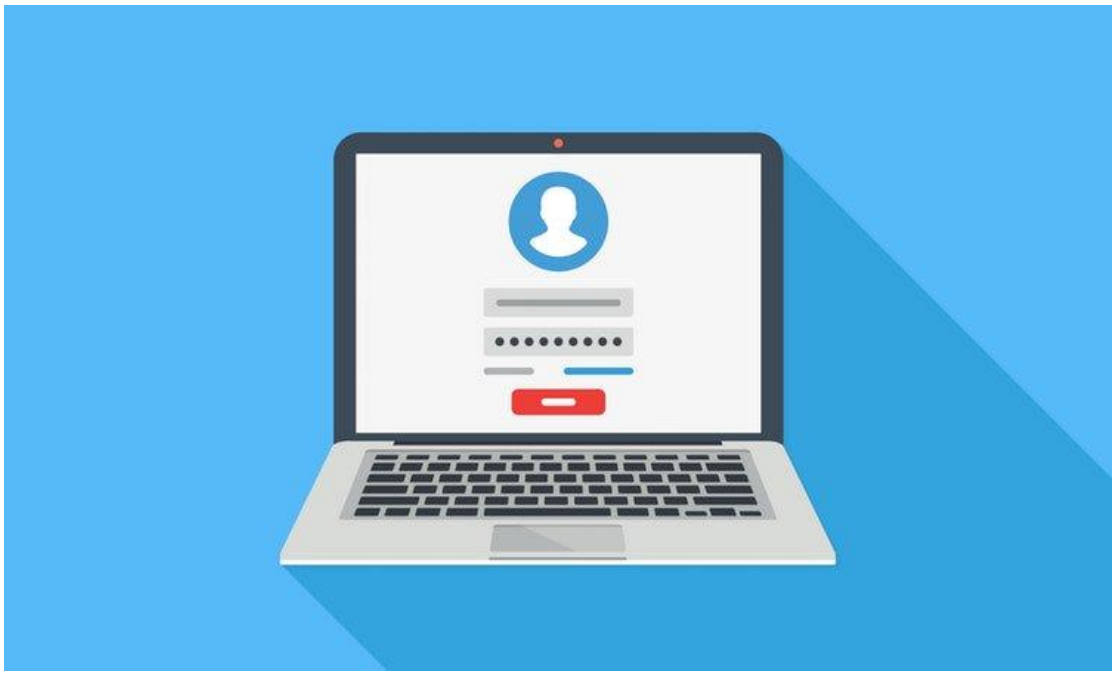
在路易斯安那州之后，过去一年中，这些类似的攻击在城市和州的袭击中显着上升，市政当局从乔治州到佛罗里达州以及美国其他地方。一种常见做法是让黑客获取并锁定城市或州的网络和文件，要求付款以扭转损害。（来源：新浪科技）

➢ 盗用会员账号非法“搬运”付费小说 10 人被刑拘

2019 年 7 月 26 日，犯罪团伙利用“黑客”技术盗取付费网站会员账号和付费小说内容，租用服务器架设多个盗版网站，为用户提供免费阅读服务，以提升网站点击量获取巨额广告

收益。7 月 25 日，记者从北京通州公安分局获悉，通州警方成功破获一起非法获取计算机信息系统数据案，抓获犯罪嫌疑人 10 名。

4 月 11 日，通州警方接到某公司报案，称其运营的网络文学网站多个会员账户被盗用，且网站部分独家授权的付费小说被他人利用技术手段非法复制，发布在其他网站上供人免费阅读，给公司造成了经济损失。接到报案后，通州分局警务支援支队立即开展调查工作。经办案民警调查发现，有上万本付费小说被转载、 2 万多个会员账户被盗，其中近 4000 个会员账户资金受损，共计 10 万余元。



民警分析这起案件的背后可能隐藏着一个专业作案团伙，利用技术手段盗取数据从事侵权牟利活动。在调查过程中，民警还发现另一家网站与被举报网站页面内容雷同，民警初步判断这两个网站为同一伙人运营。

根据报案公司提供的线索，办案民警最终追查到运营这两家网站的余某、夏某等人。4 月 29 日，通州分局民警在湖北武汉将以余某、夏某为首的 6 名犯罪嫌疑人抓获。

经审查，余某交代其伙同夏某等人，通过使用购买的专用采集器和会员账号信息，对国内多个知名小说网站的数据进行复制，并建立了多个非法网站，通过提供免费阅读小说服务吸引用户，增加网站点击量，从中获取广告费。

根据余某等人的供述，民警赴江苏宜兴将涉嫌非法获取网站会员账号并出售的蒋某某、陶某某二人抓获。该二人交代，他们从俞某某手中购买了大量网站会员账号，并在网上出售。

6 月 5 日，民警在湖北省武汉市将俞某某抓获。与此同时，另一组民警于 6 月 8 日在广东省佛山市，将涉嫌编写“黑客”程序并出售给余某获利的嫌疑人林某某抓获。至此，这个

利用“黑客”技术手段，非法获取数据、买卖公民信息、侵犯著作权等犯罪链条上的 10 名犯罪嫌疑人全部被依法刑事拘留。目前，这起非法获取计算机信息系统数据案正在进一步工作中。（来源：新浪科技）

➢ 因网站漏洞导致超过 2000 名报道 E3 记者个人信息泄漏

2019 年 8 月 4 日，在参与报道了全球最大的视频游戏大会 E3 之后，由于组织方系统存在的安全漏洞导致大量记者的个人联系信息被公开曝光。在报告中称目前已经有超过 2000 人受到影响，除了各大新闻机构和媒体的记者、编辑之外，还有 YouTube 和 Twitch 等视频网站上的网红主播，以及高盛、IMDb 和其他公司的工作人员。本周六 E3 游戏展的组织方 Entertainment Software Association（简称 ESA）向这些受影响的记者发出了电子邮件警告，而这些记者都通过官方渠道注册参与了今年 6 月在洛杉矶会议中心举办的游戏大展，并获得了新闻报道证书。

在发送给记者的电子邮件中写道：“我们为 ESA 会员和参展商在一个密码保护的参展商网站上提供了媒体列表，方便用户联系媒体进行报道，以及更好地传播参展方的展示内容。而在过去 20 多年来一直没有问题。”

在发现这个问题之后，ESA 在本周五已经发布告示称参展商网站存在缺陷，导致记者和媒体名单公布于众，随后 ESA 立即关闭了这个网站。

YouTuber Sophia Narwitz 早些时候报道了这个漏洞并注意到她已经联系了 ESA，它说可

以通过点击公共 E3 网站页面上标有“注册媒体列表”的链接来下载一份包含联系人列表的电子表格。她表示在这份名单中还包括了私人的住址信息，任何以新闻或内容创作者身份出席 E3 的人都可能受到影响。

ESA 表示：对此事件感到遗憾，并已采取措施确保不再发生这种情况。（来源：中国消费者报）

➢ 售卖企业法人精准信息数万条 一副处级干部被捕

2019 年 8 月 2 日，南京鼓楼警方通报，某省市场监督管理厅信息处主任、副处级干部郑某，因涉嫌侵犯公民个人信息罪被逮捕。经查，犯罪嫌疑人郑某利用他有权查看全国各地公司企业法定代表人个人信息的机会，伙同下线詹某、张某两人，非法售卖企业法定代表人精准个人信息，非法获利近 30 万元。

今年 2 月，南京鼓楼警方网警发现，昵称为“企业&法人”的网民在网上出售全国范围内的公司企业法定代表人姓名、身份证号码、手机号码、公司地址等非公开个人信息。通过侦查，警方发现这名网民长期活跃于湖北武汉。3 月 28 日，警方赴湖北武汉，将网名为“企业&法人”的嫌疑人詹某抓获。

据南京市公安局网安支队驻鼓楼分局大队中队长杨桂年介绍，从詹某家中的手机和电脑上面，民警现场查获尚未贩卖的公民个人信息有数十万条。

经审讯，民警查明詹某无业在家，平时靠倒卖个人信息赚钱。“然而，詹某并没有能力

直接获得法人精确个人信息，这些信息也一定是从上家处买来的。”杨桂年介绍。

通过进一步审讯，詹某交代了其上级中间商：张某，北京人，长期在互联网上贩卖公民个人信息。詹某以 20 元一条信息的价格从张某处购买，再以 35 元的价格卖出。

今年 4 月初，警方赴北京抓获嫌疑人张某。通过张某买卖企业法定代表人个人信息的分析，警方发现，泄露和买卖信息的源头，是某省市场监督管理厅信息处主任，副处级干部郑某。原来，郑某利用有权查阅全国各地企业法定代表人个人信息的机会，进行买卖。

5 月中旬，专案组民警在郑某工作单位内将其抓获归案。警方查明，自 2018 年 10 月至 2019 年 5 月，嫌疑人郑某利用职务之便，以 10 元一条的价格对外售卖。经过两层下线层层加码，最终，企业法定代表人的身份证号码、手机号码等个人精准信息，被以 35 元一条的价格对外售卖。

民警介绍，郑某的家庭条件非常优越，非法售卖个人信息只是郑某赚零花钱的手段。目前，郑某等三人因涉嫌侵犯公民个人信息罪被逮捕。

警方提醒广大市民：一定要提高安全保护意识，保管好自己的身份证、驾照、护照等证件；定时更新杀毒软件和安全管理软件；不要随意透露自己的身份信息；不要随便扫描微信二维码信息；不要随便使用公共区域的 WiFi；使用公共网络上网,下线时要清理痕迹。

（来源：看看新闻）