重磅 | 联网电力系统网络安全态势分析报告

原创：ICS-CERT 工业互联网安全应急响应中心 昨天

国家互联网应急中心 **CNCERT/CC**

北京信联科汇科技有限公司

南京莱克贝尔信息技术有限公司

摘要

CNCERT下属的工业互联网安全应急响应中心（ICS-CERT）针对我国联网电力系统的网络安全态势进行分析，2018年1-2季度期间：

1.监测发现暴露在公共互联网的电力行业网络资产1147个，其中，设备资产556个，涉及ABB、Siemens、Schneider、Delta、Rockwell等多家工控设备厂商，传统电力WEB资产532个，涉及政府监管、电力生产、电力用户以及云平台等4大类别，新能源智能电站及WEB资产59个。

2.对暴露设备资产进行漏洞巡检，发现部分设备存在严重安全漏洞，主要涉及西门子、施耐德各型号可编程逻辑控制器产品；对暴露WEB资产进行抽样漏洞巡检，发现其中超过10%的系统存在明显的安全漏洞，漏洞类型主要分为弱口令漏洞、SQL注入漏洞、代码执行漏洞、逻辑漏洞四大类。

3.CNVD漏洞库收录能源电力相关漏洞89条，其中高危漏洞51条，中危漏洞37条，低危漏洞1条，涉及SCADA系统、可编程逻辑控制器、HMI、工业网络设备、工业应用软件等多种类型的软硬件产品。

4.监测到来自境外重点探测组织的IEC-104、Modbus等电力协议相关的端口探测事件共2880316起，涉及到境外81个IP地址，分布在美欧地区；抽取84个暴露在公网的重要WEB电力监控管理系统进行了为期1周的全流量监测，发现1486次来自境外的木马注入、权限获取等网络攻击事件。

5.通过引入联网电力系统网络安全威胁指数，从设备资产和WEB资产两个角度，结合漏洞威胁等级、探测次数和攻击次数，对我国不同地区的联网电力系统安全威胁指数进行了综合分析，发现多数省份情况良好，而广东、北京等省市安全形式相对严峻。

目录

1 前言

1.1电力行业背景

电力行业是国民经济发展中最重要的基础能源产业，是经济发展和社会进步的基石。作为一种先进生产力和基础产业，电力行业不仅对国民经济的发展起到至关重要的作用，而且与人们的日常生活、社会的稳定息息相关。电力行业基本上可以划分为发电、供电两大系统和发电、变电、输电、配电、用电五大环节。发电系统根据电厂的发电能级以及所处的位置又可以分为跨网电厂、网级电厂、省级电厂、自备电厂及小型电厂四个发电级别，统一向电网供电。供电系统实行分层管理，可以分为国家电网公司与中国南方电网公司、各区域电网公司、各省电力公司及各市区县供电公司等。发电厂将火力、水力、核能、风能等原始能源转换为电能后，通过升压经由输电线路传输到负荷区域，后通过降压经配电线路输送到各公用配电间，再降压最终输送到用电用户。电力输送流程如图1.1和图1.2所示。

图1.1 电力输送流程图

图1.2电力系统示意图

1.2电力系统网络安全

随着我国电力系统的网络化和智能化发展，其主要面临以下几个方面的网络安全威胁和挑战：

- 感知层安全

电力系统中存在大量的智能感知设备，这些设备通常情况下功能单一、计算和存储能力有限，无法应用复杂的安全防护技术。攻击者可以直接通过网络访问智能仪表、传感器等感知设备的内存数据进行攻击，进而读取诊断端口等敏感信息。此外，攻击者还可以对网络接入点进行嗅探和窃听，破解加密网络捕获智能仪表中的保密性数据。另外，还可以对智能仪表进行干扰和访问限制，以及盗窃攻击等。

- 协议层安全

电力系统中涉及到多种类型的设备，这些设备使用种类繁多的通信协议以及电力系统专属网络协议，包括DNP3、Modbus、ICCP/TASE.2、PROFIBUS以及CIP等，它们完成了电力系统的数据采集交换、命令发布与执行、业务监控与管理等诸多重要功能。然而这些协议从颁布至今已经运行数十年，随着电力系统的发展其安全问题日益突出。许多协议缺少认证机制且没有必要的加密措施，使得电力系统很容易遭受网络攻击。

- 网络层安全

由于电力系统对网络的严重依赖性，系统极有可能遭受暴力破解攻击、欺骗攻击、中间人攻击、拒绝服务攻击等非法攻击。例如：通过冒充仪表在网络中的身份进行攻击，或者攻击方将自身连接到通信设备之间窃取或篡改网络通信数据，或者通过耗尽电网网络的计算资源，阻断正常的通信和服务，以此影响正常的系统运行。

- 硬件层安全

电力系统中部署大量的服务器、工作站、交换机、路由器、可编程逻辑控制器等硬件设备。考虑到设备功能的复杂性，硬件和对应的固件系统中难以避免存在一些漏洞，如果未能及时修补则很容易被利用和攻击。此外，电力系统中的设备为了方便管理和使用，出厂设置中默认开启了一些网络服务，如HTTP服务、Telnet服务、FTP服务，或者提供了一些缺省的网络设置，如缺省的SNMP信息等，这些情况将会造成设备的信息泄露，进而引发有针对性的攻击行为。

- 软件和应用层安全

电力系统中应用了大量IT通用软件，以及电力专用软件，其涉及的操作系统、业务软件、数据库、以及中间件等都可能存在设计缺陷和漏洞。当管理系统尤其是生产管理系统与互联网连接时，攻击者可通过利用漏洞向电力系统植入病毒、木马等恶意软件进而窃取系统中的重要信息和数据，或尝试控制和破坏系统。

- 数据层安全

在电力系统中数据安全的含义有两点：一是数据本身的安全，即数据加密、数据完整性保护、数据访问控制等存在隐患。例如，电力系统中智能仪表通信通常缺少加密认证机制，不仅会泄露用户的用电量，也可能泄露用户重要的隐私数据，攻击者利用这些信息可以推断出用户的日常活动。二是数据存储的安全，如数据中心、容灾备份等数据安全防护存在隐患。

当前，电力系统的信息网络正从“大型、封闭”网络逐渐转换成“超大型、半封闭”网络，随之引发了新的联网安全问题，继电保护、电网调度自动化和安全装置、变电站自动化、发电厂控制自动化、配网自动化、电力市场交易、电力负荷控制、电力用户信息采集、智能用电等多个环节的电力网络资产由于设计需求或配置错误，都有可能暴露在公网之中，使电力系统原有的安全问题愈发突显，对原先以物理防护为主的电力安全防护体系带来了更大的挑战。

2 电力行业网络安全事件

2.1国外安全事件

2018年3月21日，黑客攻占了印度 Uttar Haryana Bijli Vitran Nigam（UHBVN）电力公司的计算机系统，窃取了用户的账单数据，导致电力公司无法对用户之前的用电量进行计算。攻击者对电力公司进行了勒索，索要一个 1 RS Core 或者 1000 万卢比才肯归还数据。

2.2国内安全事件

2018年3月28日11时45分，**省电力调度控制中心内网安全监控平台出现大量告警，且告警数量急剧增加。经分析确认，告警信息为**某风电场省调接入网非实时纵向加密认证装置拦截的不符合安全策略的非法访问，观察一段时间后发现告警数量不断增加并无减少迹象。**省电力调度控制中心按照网络安全防护应急处置措施，要求现场立即断开风功率预测服务器与调度数据网及站内电力监控系统的全部物理连接，告警信息消失。事件发生后，**省电力调度控制中心派技术人员现场调查，发现导致本次网络安全事件的原因为厂家对功率预测服务器进行远程运维，开启了文件共享等功能。该站长期将电力监控系统生产控制大区裸露于公网，给电网安全运行带来极大隐患。

3 电力行业网络资产暴露情况

3.1电力行业设备资产暴露情况

2018年第1~2季度，ICS-CERT监测发现全国网络空间范围内使用IEC104、Modbus、EtherNet/IP等协议（以上协议为电力行业设备广泛使用的通信协议）的能源电力行业联网设备556个，涉及到大量西门子、施耐德、ABB、罗克韦尔等企业生产的能源电力相关产品，例如西门子的

S7-200、S7-400，施耐德的TWDLCAA40DRF、BMX P34 2020、TM221CE16R等型号的可编程逻辑控制器。

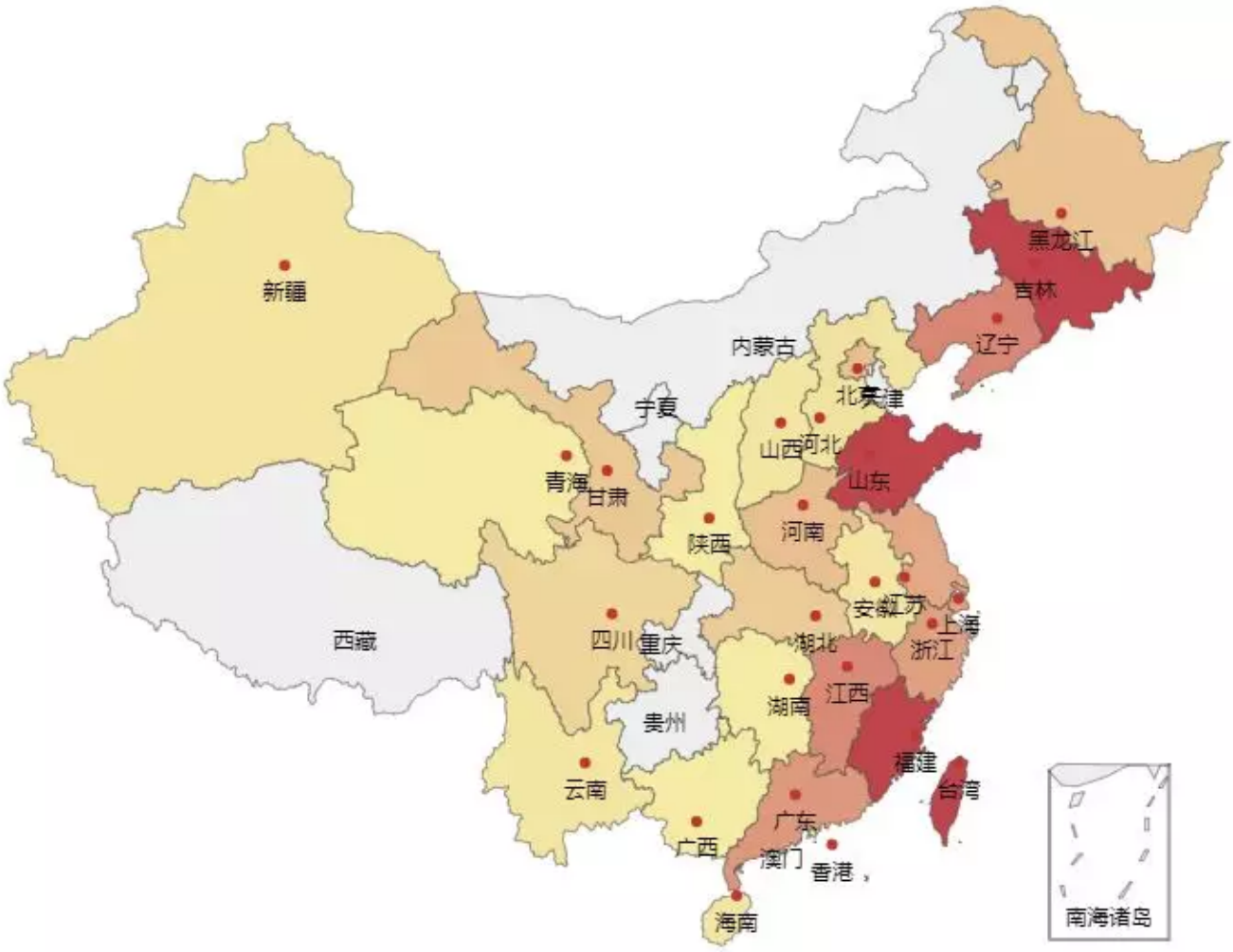

图3.1 暴露电力设备的全国分布图

如图3.1所示，这些设备分布在全国27个省市中，其中数量排名前五的省市分别为台湾（172）、吉林（76）、山东（67）、福建（50）、辽宁（24）。通过网络基础信息查询，对部分暴露设备的归属及用户信息进行了识别，例如，查询发现部分暴露设备隶属于临沂**公司**充电站、瓜州**风电场等电力企业。

除了上述IEC104、Modbus、EtherNet/IP等协议，电力行业中还存在其它专用协议，例如IEC103、IEC101、IEC92、IEC-MMS等协议，构成了电力系统自动化全球通用标准。但在本次巡检过程中，没有发现使用以上协议的互联网暴露设备资产。

3.2电力行业WEB资产暴露情况

2018年第1~2季度，ICS-CERT监测发现全国大量电力行业相关的联网WEB资产，从传统电力WEB资产和新能源电站WEB资产两个维度进行统计，具体情况如下。

3.2.1传统电力WEB资产暴露情况

发现的传统电力WEB资产主要分五种类型：政府监管平台、电力企业相关平台、用电管理平台、云平台以及企业门户网站。由于绝大部分电力企业门户网站都托管在专业机房以及云服务平台中，不存在与生产环境的直接联系，故本报告不做重点分析。

此次发现暴露在公网上的传统电力WEB资产共计523个，其中政府监管平台79个（涉及国家电力需求侧管理平台、能源管理系统、能源监督系统等）、电力企业相关平台406个（涉及电表充值系统、充电桩管理系统、电能管理系统、风电场监测系统、供电巡检管理系统、光伏电站监控系统以及企业内部管理系统等）、用电管理系统6个（涉及能耗检测系统以及用电管理网上查询系统）以及云平台32个（发电机组云控平台、分布式光伏电站智能管理系统、电力智能云管理系统、企业能源管理云平台等）。

详细分类见图3.2和表3.1。

图3.2暴露的传统电力WEB资产的分类

表3.1暴露的传统电力WEB资产的分类统计

一级分类	二级分类	数量
政府监管平台	需求侧管理平台	22
	能源管理系统	14
	能源监督平台	27
	电力业务许可平台	4
	其他	14
	企业内部管理系统	48

电力企业相关平台	充电桩管理系统	38
	企业服务平台	28
	企业邮件系统	26
	能源监控系统	25
	风电场监测系统	18
	电能管理系统	17
	企业信息管理系统	17
	能源管理系统	15
	变电站管理系统	14
	用电管理系统	11
	光伏电站监控系统	8
	工程管理平台	6
	电表充值系统	5
	供电巡检管理系统	4
	企业MIS系统	4
	特变电管理系统	4
	气象环境监测系统	3
	其他	115
用电管理平台	能耗检测系统	3
	用电管理网上查询系统	3
云平台	发电机组云控平台	1
	分布式光伏电站智能管理系统	10
	电力智能云管理系统	2
	企业能源管理云平台	5
	充电云平台	7
	其他	14

这些WEB资产分布于全国30个省、直辖市或自治区。选取出其中TOP 15如图3.3所示，北京、长三角和珠三角等经济发达地区暴露WEB资产最多，其亦为电力消费大省，此外，重要能源省份也有大量暴露电力WEB监控管理系统。

图3.3暴露的传统电力WEB资产的地区分布（TOP15）

3.2.2新能源电站WEB资产暴露情况

我国政府高度重视可再生能源的研究与开发。根据2014年数据，中国新能源发电累计并网容量突破1亿kW，占全部发电装机容量的9.8%。中国新能源发电量约为2190亿kW·h，同比增长18%，约占全部发电量的3.9%。其中风电发电量1563亿kW·h，太阳能发电量208亿kW·h，其他新能源发电量约418亿kW·h，分别占新能源发电量的71%、10%、19%。可见新能源在我国能源结构中占据越来越重要的比例，新能源电站的安全问题也越来越值得关注。

ICS-CERT通过对互联网中的新能源电站天气查询数据流量进行监测分析，共发现新能源智能电站及部分WEB资产相关IP共59个，如图3.4。

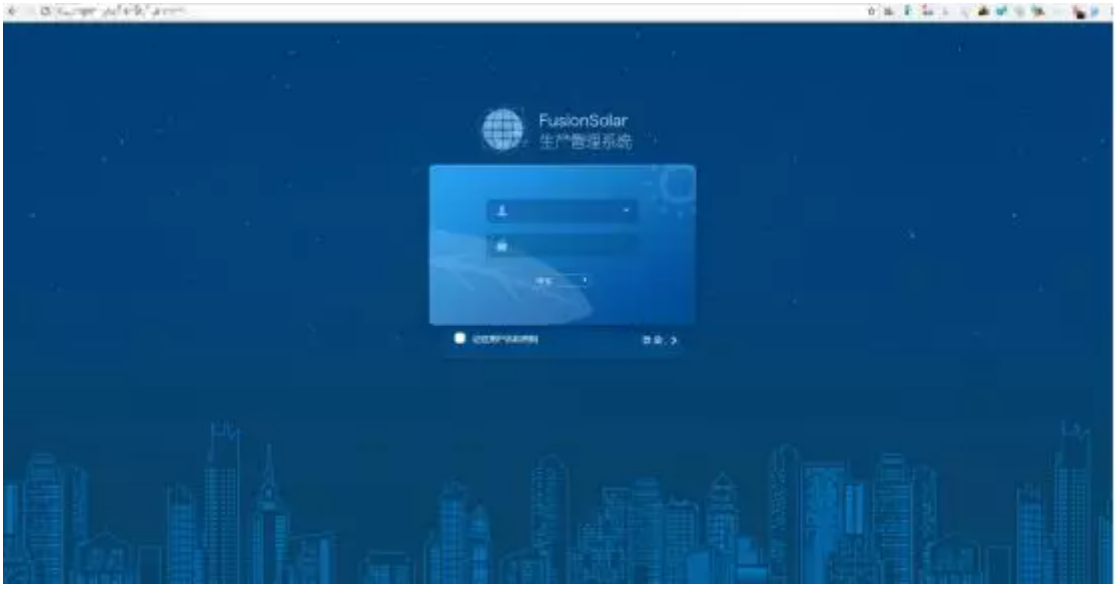

图3.4 FusionSolar生产管理系统

图3.5和表3.2显示，发现的新能源电站主要分布在我国的新疆、西藏以及宁夏地区。这些地区位于我国中西部，太阳能和风能资源丰富，地广人稀，便于发展大规模的清洁能源产业。

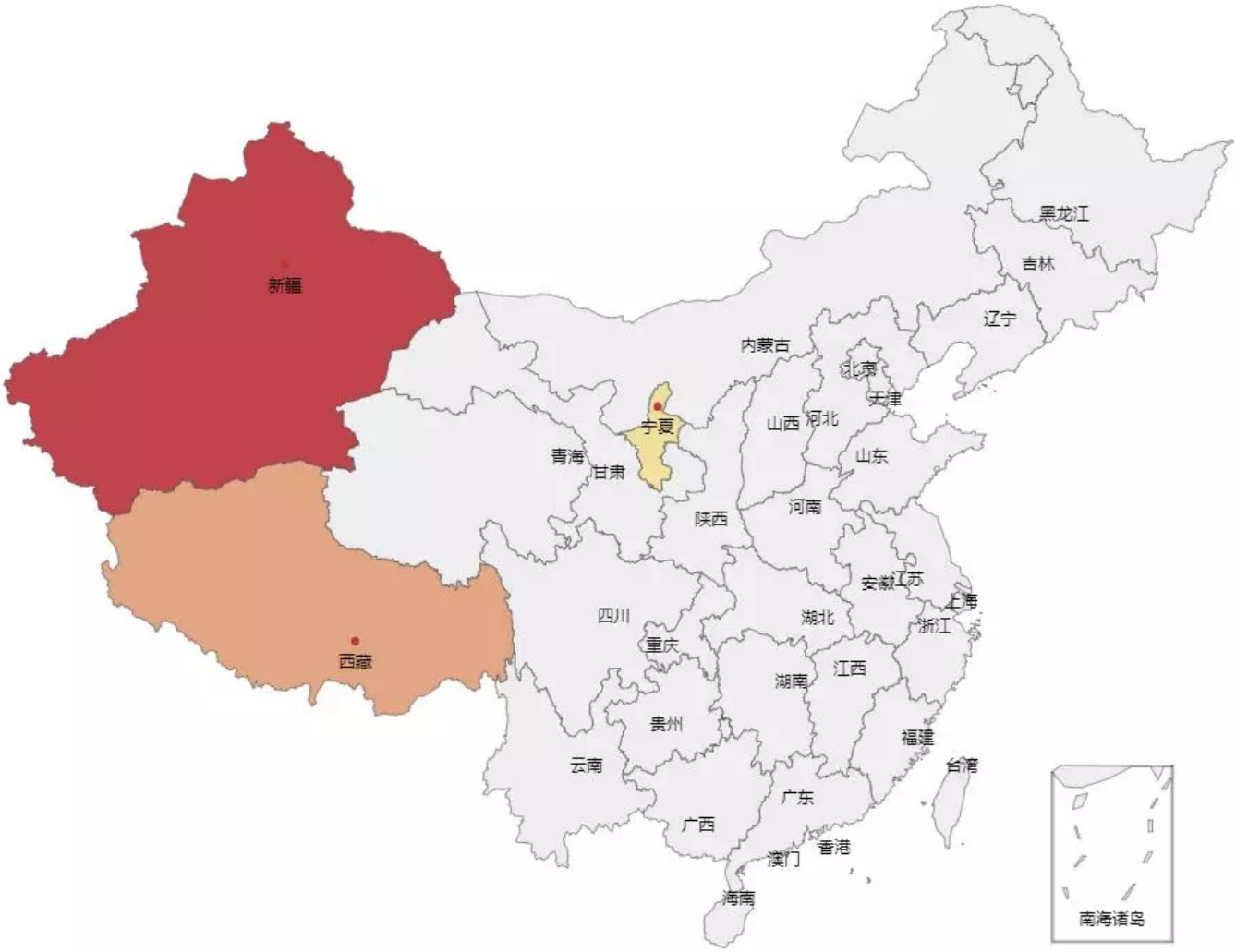

图3.5 新能源智能电站分布图

表3.2 发现的新能源电站IP数量按省市排名

省市	新能源电站IP数量
新疆	53
西藏	5
宁夏	1

通过网络基础信息查询，显示这些IP分别属于宁夏**新能源基地、**变电站、新疆哈密**能源、新疆昌吉**以及新疆哈密**风电公司等新能源企业。

4 电力行业网络安全漏洞风险分析

4.1暴露设备资产的漏洞巡检情况

将3.1节中发现的暴露设备的基本信息与CNVD漏洞数据库进行比对，发现其中部分型号的设备存在安全漏洞，主要涉及Siemens生产的S7-400（7个漏洞）、S7-200（2个漏洞）、施耐德生产的

BMX342020（2个漏洞）、TSXETY103（1个漏洞）、TM221CE16R（2个漏洞）、BMXNOE0100（2个漏洞）。

表4.1 暴露设备的漏洞统计

产品型号	生产厂商	暴露数量	漏洞编号	漏洞等级
SIMATIC S7-400	Siemens Electric	6	CNVD-2012-4031	高
			CNVD-2016-12695	中
			CNVD-2016-12694	中
			CNVD-2017-06153	中
			CNVD-2017-06151	中
			CNVD-2018-06025	中
			CNVD-2012-4032	高
BMX NOE 0100	Schneider Electric	35	CNVD-2011-5607	高
			CNVD-2015-08446	高
BMX P34 2020	Schneider Electric	38	CNVD-2011-5607	高
			CNVD-2015-08446	高
TSXETY4103	Schneider Electric SAS	21	CNVD-2011-5607	高
SIMATIC S7-200	Siemens	62	CNVD-2017-06153	中
			CNVD-2017-06151	中
TM221CE16R	Schneider Electric	1	CNVD-2017-05014	高
			CNVD-2017-05011	中

4.2暴露WEB资产的漏洞巡检情况

抽取了200个3.2节中发现的暴露WEB资产，其中生产管理类系统127个，生产监控类系统73个。通过对这些系统进行远程安全巡检，发现其中共有21个系统存在严重安全漏洞隐患，即有超过10%的系统存在明显的安全问题，其中生产监控类16个，生产管理类5个。

在安全巡检过程中，共计发现35个安全漏洞，其中高危漏洞24个，占比达到68.6%。我们对WEB系统存在的安全漏洞进行了简单的归类与统计分析，按照漏洞类别归类，主要包括四大类：弱口令漏洞、SQL注入漏洞、代码执行漏洞、逻辑漏洞等。其中被红色标记的弱口令、SQL注入、代码执行等属于高危漏洞，攻击者利用此类漏洞可获取WEB系统甚至服务器的控制权。此外，逻辑漏洞所包含的种类比较多，不仅包含路径遍历漏洞这类对输入解析不完善导致的漏洞，诸如认证机制隐患、访问控制缺失、防护机制隐患等漏洞与具体的WEB实现逻辑相关，比较混杂，很难有一个明确而具体的分类，因此也将其统一划归到逻辑漏洞这个宽泛的类别下。

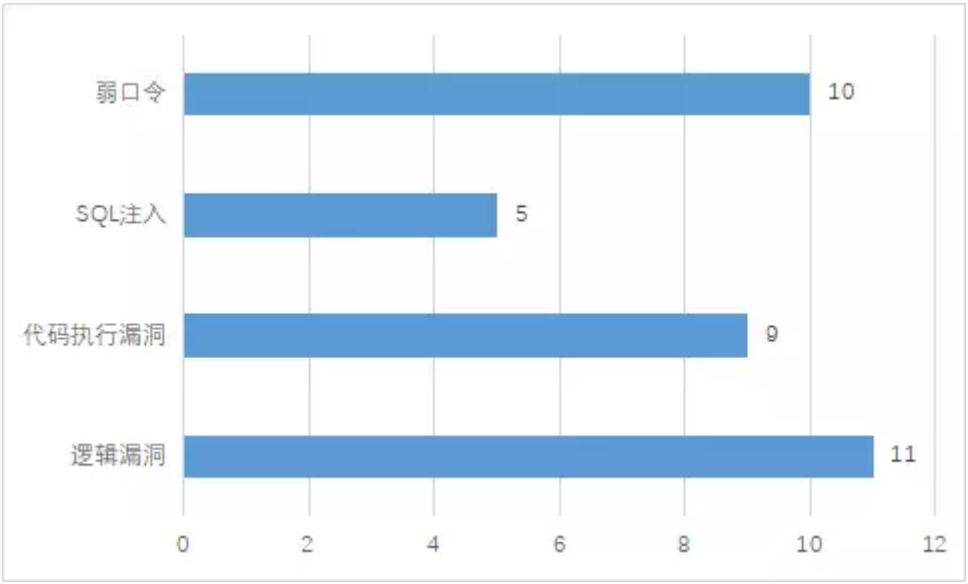

图4.1 WEB系统漏洞巡检结果及分类

以下是针对WEB资产高危漏洞的验证案例：

1) 弱口令漏洞

弱口令漏洞在所有工业控制系统中都不罕见。工控企业运维人员普遍存在网络安全意识淡薄的问题，这已成为工控网络安全问题频出的最大诱因。工控运维人员在日常的运行维护中，暴露出很多低级别错误，例如大量使用的弱口令。根据我们发现的情况，常用的弱口令组合包括admin/000000、admin/admin、test/123456、test/test、test1/test1、admin/12345。攻击者利用弱口令可直接进入生

产类系统，轻则造成大量生产数据、用户数据被窃取，重则导致生产系统被操纵，生产活动被干扰或破坏。

下面给出针对电力行业WEB系统安全巡检中发现的典型实例，即陕西省某能源公司风力发电机组信息管理系统。

该系统主要负责风力发电系统的信息化管理，包含风场监控、风机监控、报表生成等功能。目前发现该服务器上8000端口开放了Tomcat的管理服务，其中存在弱口令漏洞，可以直接植入后门，控制整个服务器。同时8000端口上开放的盾安风场监控管理系统，同样存在弱口令漏洞，系统中泄露了内网中风机IP地址等相关信息。

图4.2 某能源公司风力发电机组信息管理系统

2) SQL注入漏洞

SQL注入漏洞是最常见的WEB漏洞，产生原因通常是程序员没有对输入参数做好过滤。SQL注入漏洞属于高危漏洞，造成的危害通常包括泄露敏感信息、提升权限、操作任意文件、执行任意命令等。

下面给出针对电力行业WEB系统安全巡检中发现的典型实例，即河北省某电厂巡检系统。

该系统登录界面存在SQL注入漏洞，远程攻击者可绕过密码限制登录系统，获取生产信息等敏感数据。

图4.3河北省某电厂巡检系统

3) 代码执行漏洞

我们发现的代码执行漏洞包括服务器存在的HTTP.sys RCE漏洞（CVE-2015-1635）漏洞，数据库存在的命令执行漏洞以及网站存在的Struts2系列漏洞（S2-016、S2-032、S2-045等）。特别是Struts 2漏洞，近年来层出不穷，需要格外关注。代码执行漏洞会导致攻击者在目标系统执行任意命令，属于高危漏洞。

下面给出针对电力行业WEB系统安全巡检中发现的两个典型实例，一是陕西省某发电公司SIS系统，另一个浙江省某热电厂管理信息系统。

该SIS系统包括生产过程管理、数据查询、报表查询、性能计算、数据运维等功能，其中核心的是生产过程管理和数据查询功能。该系统存在Struts2 S2-019远程代码执行漏洞，远程攻击者利用这些漏洞可以直接控制服务器，获取大量敏感信息，进而进行内网漫游，伪造传感器信息，干扰工控设备运行，破坏生产活动。

图4.4陕西省某发电公司SIS系统

图4.5 进入内网后可以直接控制生产设备参数

在浙江嘉兴某热电厂管理信息系统这个案例中，攻击者可利用该漏洞去控制该热电厂的管理信息系统，进而对内网进行攻击和渗透，最严重的情况是该电厂停摆，造成区域停电事件。

攻击方式如下，添加一个名为hacker密码123456的用户，则可以执行命令（http://xx.xx.xx.xx:8080/.../.../.../.../windows/system32/cmd.exe?/c+net+user+hacker+123456+/add）。由于该服务器还打开了3389端口，因此如果攻击者将新建的管理员账户添加到远程用户组，就可以直接通过windows远程桌面登录到该服务器，获得完整控制权。

图4.6 电厂管理信息系统的截图

4) 逻辑漏洞

逻辑漏洞包含的种类非常多，和登录认证相关的就包括验证码缺失或绕过、登录绕过、验证逻辑不合理等漏洞，本次针对电力行业WEB系统安全巡检过程中发现的问题主要集中在登录认证部分。

巡检中发现，存在的主要问题有三类：

① 登录界面没有验证码机制，导致可被暴力破解；

②用户名和口令传输过程没有加密；

③登录界面的验证码机制可以很轻易地绕过。

下面给出安全巡检中发现的典型实例，即四川省某供电公司输配电线路故障在线监测系统。

该系统存在未授权访问漏洞、登录绕过漏洞和信息泄露漏洞，远程攻击者利用这些漏洞可以控制服务器，获取敏感信息，破坏生产活动。

图4.7 线路信息可被直接访问

图4.8 用户名和口令明文保存

4.3电力行业产品漏洞情况

4.3.1产品漏洞总体情况分析

ICS-CERT/CNCERT下属的国家信息安全漏洞共享平台（CNVD）在第1~2季度共收录89条能源电力行业相关产品漏洞，其中高危漏洞51条，中危漏洞37条以及低危漏洞1条。

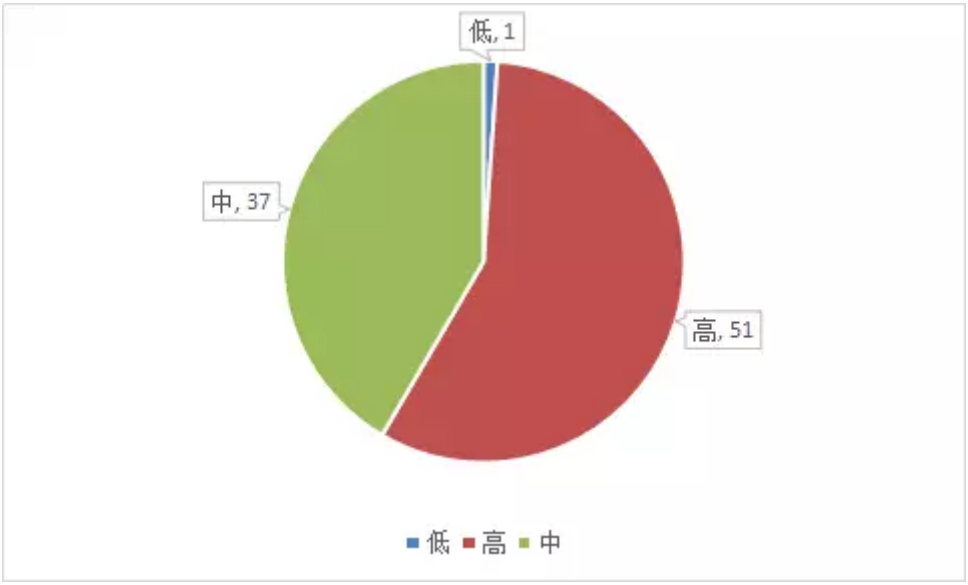

图4.9 漏洞等级分布图

表4.2和4.3统计显示，这些漏洞影响到包括研华、欧姆龙、西门子、台达等多家厂商，涉及到SCADA系统、工业应用软件、可编程逻辑控制器、HMI、等多种类型的软硬件产品和服务。

表4.2厂商漏洞数量统计表

厂商	漏洞数量	厂商	漏洞数量

研华	17	WAGO	2
西门子	14	英威腾	1
台达电子	8	伊顿	1
欧姆龙	7	罗克韦尔	1
施耐德	6	Sprecher	1
Geutebrück	6	Rapid	1
和利时	4	Nari	1
ABB	4	Moxa	1
WECON	3	MatrikonOPC	1
Martem	3	LCDS	1
GE	3	3S-Smart	1
横河电机	2		

表4.3漏洞涉及产品类型统计表

产品类型	漏洞数量	产品类型	漏洞数量
工业应用软件	28	工业路由器	7
SCADA	26	能源楼控系统	3
HMI	11	网络通信模块	3
工业交换机	2	PLC	8
智能控制器	1		

4.3.2典型高危产品漏洞影响评估

ICS-CERT对1~2季度涉及能源电力行业软硬件产品的部分重点高危漏洞进行了分析评估，对其涉及的联网资产进行了互联网暴露情况排查，重点包括：

- CNVD-2018-12127漏洞（评分为8.6）

影响的设备为罗克韦尔自动化公司研发的CompactLogix 5370 系列控制器，其存在不恰当的输入验证漏洞，成功利用此漏洞可导致设备处于拒绝服务状况。ICS-CERT经监测发现了20台受到该漏洞影响的在线设备，分布在上海、山东、浙江、台湾等地。

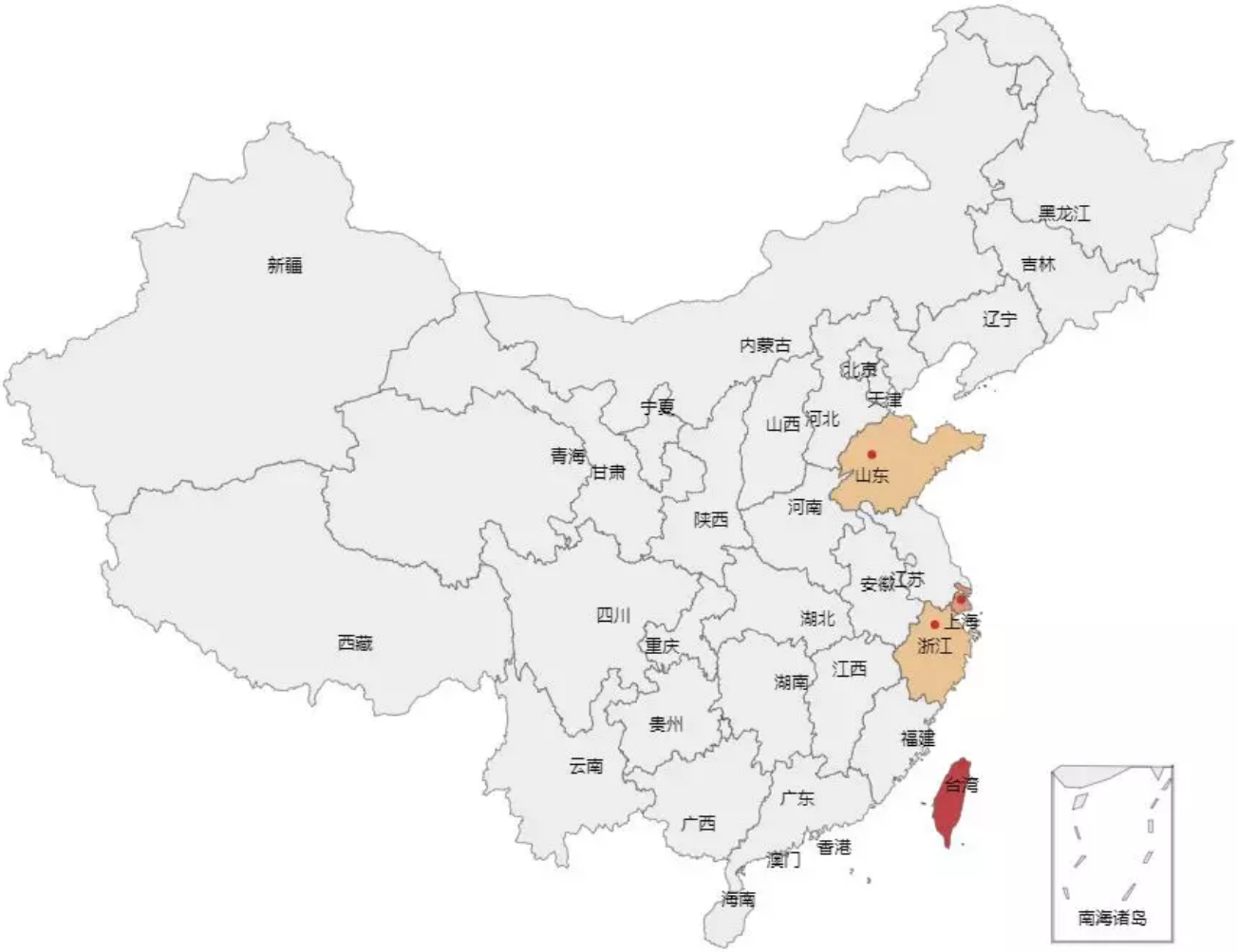

图4.10 CNVD-2018-12127漏洞相关设备的全国在线分布

- CNVD-2018-08447漏洞（评分为9.8）

影响的产品为法国施耐德电气公司研发的InduSoft Web Studio和InTouch Machine Edition嵌入式HMI软件包。其被发现存在可利用的缓冲区溢出漏洞，攻击者在读取和写入标签、警报或与事件相关的操作期间，可远程发送精心设计的数据包，利用该漏洞在服务器中执行任意代码。经ICS-CERT经监测发现了7个受到该漏洞影响的在线产品，分布在北京、浙江、广东、香港等地。

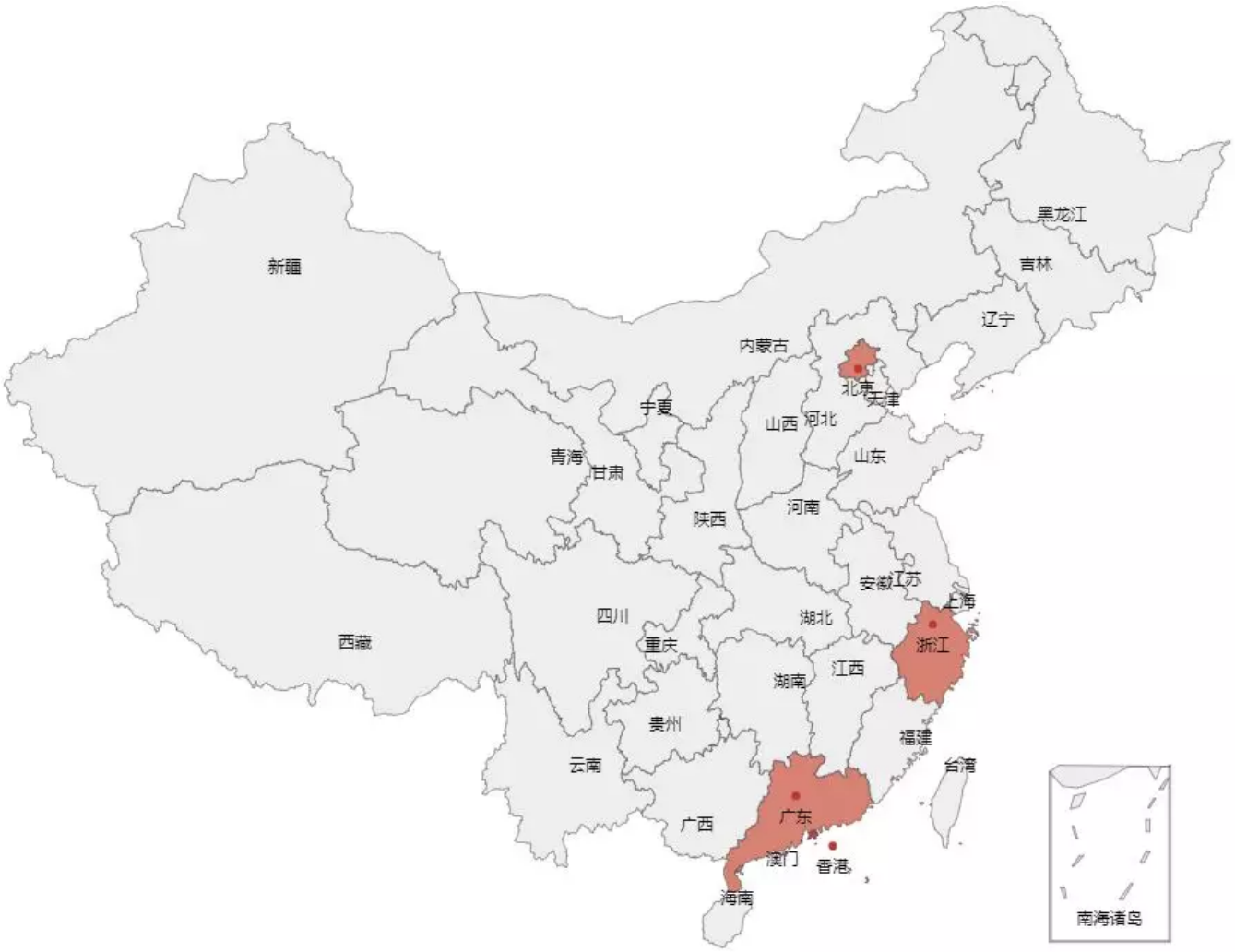

图4.11CNVD-2018-08447漏洞相关产品的全国在线分布

5 电力行业网络安全监测情况

5.1跨境端口探测情况

2018年第1~2季度，ICS-CERT累计监测到来自境外重点探测组织的IEC-104、Modbus等电力协议相关的端口探测事件2880316起，探测事件趋势如下图所示。

图5.1 探测事件趋势图

在监测到的探测数据中，按照探测次数统计，排名前5的省市分别为：广东（672149次）、北京（328942次）、江苏（289766次）、浙江（266515次）和香港（245794次）。如图5.2所示。

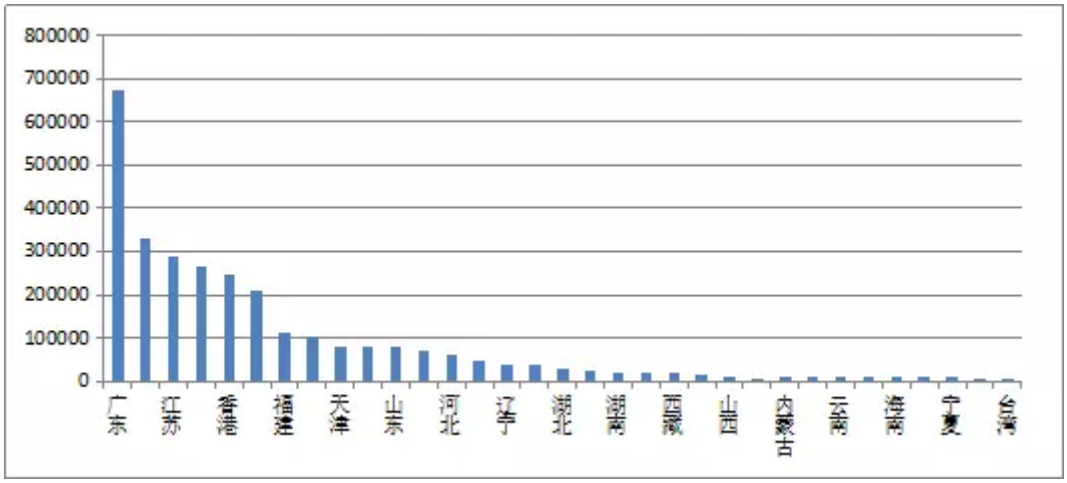

图5.2 探测事件次数按地区统计

重点探测组织涉及到境外81个IP地址，分布在美国（75个）、荷兰（4个）和冰岛（2个）3个国家。经分析，这些节点隶属于Shadowserver、Shodan、密西根大学等机构，其利用IEC104协议、Modbus等电力相关协议对境内开展长期、持续、大范围的扫描探测。

5.2跨境网络攻击抽样监测情况

ICS-CERT针对84个暴露在公网的典型WEB电力监控管理平台进行了为期1周的抽样监测，发现木马注入类型攻击（947次）、管理员权限获取类型攻击（518次）、潜在企业隐私侵犯攻击（3次）、WEB应用攻击（3次）以及Asterisk 拒绝服务攻击（15次）共计1486次，涉及平台数量43个，占抽样监测平台总数的51.2%。表5.1展示了针对各类电力监控管理平台攻击事件的统计情况。

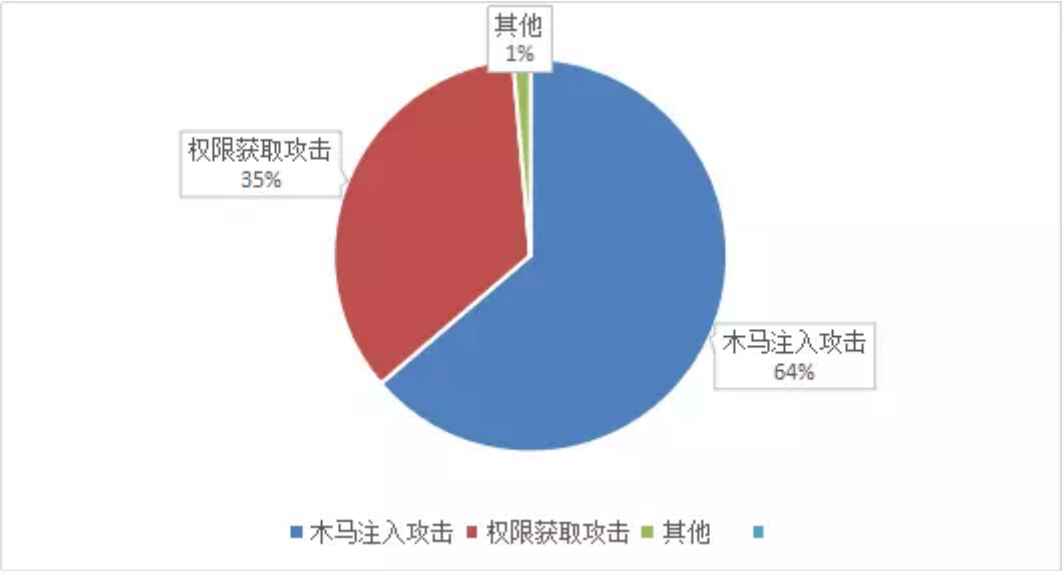

图5.3 攻击类型分布

表5.1 针对各类电力监控管理平台攻击事件的统计

被攻击平台一级分类	被攻击平台二级分类	攻击次数
政府监管平台	能源管理系统	786
	需求侧管理平台	8
	能源监督平台	8
电力企业相关平台	光伏电站监控系统	83
	电能管理系统	42
	风电场监测系统	24
	充电桩管理系统	10
	能源管理系统	10
	电表充值系统	4
	其他	4
	用电管理系统	3
用电管理平台	能耗监测系统	394
云平台	电力智能云管理系统	37
	企业能源管理系统云平台	17

由此可见，暴露在互联网上的电力相关平台真实存在被跨境网络攻击的风险，其攻击源IP地址分布在多个国家，其中排名前五的国家为墨西哥（72个）、俄罗斯（64个）、美国（18个）、巴西（13个）以及日本（5个）。

如图6.1所示，为分析得到联网电力系统安全态势，首先分别计算联网电力设备资产安全威胁指数和联网电力WEB资产安全威胁指数。两类指数计算的原理类似，计算过程中重点考虑暴露资产的漏洞威胁和暴露程度两方面的因素。最后将设备和WEB两类威胁指数综合加权，进而形成联网电力系统网络安全威胁综合评估指数及安全态势。

图6.1联网电力系统网络安全态势评估体系

6.1联网电力设备资产安全威胁评估分析

针对监测发现的联网电力设备资产，以省、自治区和直辖市作为评价对象，首先分别计算各个地区的联网设备漏洞评估指数和联网设备暴露评估指数，漏洞威胁评估主要参考联网设备的漏洞巡检结果和CNVD漏洞威胁评分，如果某个设备存在多个漏洞，则以威胁等级最高的漏洞为准；暴露程度评估主要参考设备资产所在地区被扫描探测的次数以及被尝试攻击的次数，如果某个地区被扫描探测和攻击的次数越多，则说明该地区暴露程度越大，漏洞从威胁转为安全事件的可能性就越大。将各个地区的漏洞评估指数和暴露评估指数分别做归一化处理，并将两者相乘即得到各个地区的联网电力设备资产安全威胁指数，如图6.2所示。

图6.2 各地区联网电力设备资产安全威胁评估指数

通过分析发现，我国主要工业大省（如广东省、山东省、江苏省、浙江省）和政治经济中心（北京市和上海市）的联网电力设备均面临相对较高的网络安全风险，这些重点省市同时也是电网的核心组成部分。

6.2联网电力WEB资产安全威胁评估分析

针对监测发现的联网电力WEB资产，采用相同的方法计算各个地区的联网电力WEB资产安全威胁指数，如图6.3所示，与联网设备资产不同的是北京市的电力WEB资产安全威胁相对更加突出。推断是由于北京作为我国行政中心，有大量存在漏洞安全隐患的电力监控管理系统暴露在公网。

图6.3 各地区联网电力WEB资产安全威胁评估指数

6.3联网电力系统网络安全威胁综合评估分析

按照6.1节叙述的方法，将设备和WEB两类威胁指数综合加权（由于设备涉及底层生产过程，其权重可适当调高），即得到我国各个地区联网电力系统网络安全威胁综合评估指数，如图6.3所示。

图6.3 各地区联网电力系统安全威胁综合评估指数

进一步将综合威胁指数分为5个等级：优（0-0.2）、良（0.2-0.4）、中（0.4-0.6）、差（0.6-0.8）、危（0.8-0.1），据此得到了全国联网电力系统综合安全态势。图6.4显示，广东省、北京市以及沿海省份联网电力系统安全形势相对严峻，是网络攻击潜在的重点目标区域。

图6.4 我国联网电力系统综合安全态势

7 总结和建议

针对联网电力系统暴露的若干网络安全问题，ICS-CERT认为，应该在以下几个方面进行进一步的改善。

隔离：从报告数据中可以看到，仍有不少电力设备或系统暴露在互联网上，需要重点分析和整改。进行隔离的主要目的就是最小化被攻击的影响，如通过地理位置来隔离电网部署、禁止不同位置不同区域间的通信等。通过更为严格的隔离措施，阻止病毒入侵，或使得病毒或者其他攻击行为只能存在于其最初进入的位置而不扩散。

代码和命令签名：电力设备的软件开发者必须对他们的代码以及接受或发送数据的关键命令实施签名。代码签名和命令签名可利用哈希等算法来验证代码的完整性。如果不实施相关操作，攻击者可以能在智能设备上执行任意代码造成不可知的风险。

安全评估和渗透测试：通过漏洞扫描、脆弱性评估等安全评估方式去识别、量化和给脆弱性等级排序，结合渗透性测试方法，利用被识别的漏洞和威胁来评估其面临的风险。电力企业应针对系统内包含敏感信息或是关键基础设施的环境进行测试。应聘请或建设专业安全评估队伍和渗透测试专家长期对关键环境进行评定。

日志和监控：为了处置在遭受攻击后无法溯源的状况，电力企业应建立完善的日志和监控措施，用以识别攻击以及在安全事件发生后重构事件。监控的能力不仅应包含电力环境中的敏感信息和关键基础设施部分，还应扩展到应用程序、操作系统和网络级别。