国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 12 月 19 日-2022 年 12 月 25 日 **2022 年第 51 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

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 614 个，其中高危漏洞 283 个、中危漏洞 290 个、低危漏洞 41 个。漏洞平均分值为 6.46。本周收录的漏洞中，涉及 0day 漏洞 463 个（占 75%），其中互联网上出现“Advantech iView SQL 注入漏洞、Egavilan Media Resumes Management and Job Application Website SQL 注入漏洞”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 36292 个，与上周（26350 个）环比增加 0.38 倍。

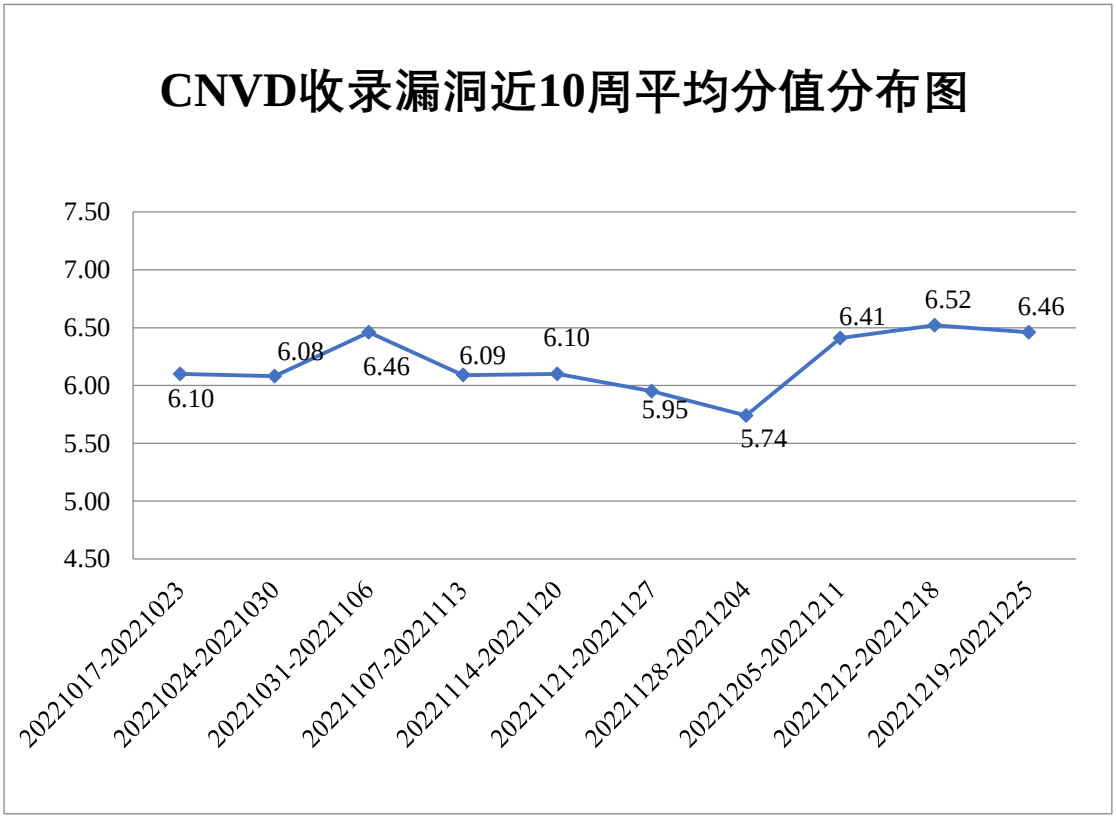

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 13 起，向基础电信企业通报漏洞事件 28 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 646 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 112 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 62 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

重庆中联信息产业有限责任公司、重庆米未科技有限公司、重庆猫扑网络科技有限公司、重庆劳格科技有限公司、中企动力科技股份有限公司、中联重科股份有限公司、中科宇图科技股份有限公司、中孚信息股份有限公司、政和科技股份有限公司、浙江中控技术股份有限公司、浙江诺诺网络科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江华途信息安全技术股份有限公司、浙大恩特网络科技有限公司、掌淘网络科技（上海）有限公司、长沙米拓信息技术有限公司、鱼跃 CMS、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、医兰达(深圳)网络科技有限公司、研华科技（中国）有限公司、亚信科技（成都）有限公司、信呼、新道科技股份有限公司、西安众邦网络科技有限公司、西安思铂电子科技有限公司、西安市利谱信息技术有限公司、西安瑞友信息技术资讯有限公司、西安瑞箭软件有限公司、武汉思维跳跃科技有限公司、武汉市华科兄弟数字技术有限公司、武汉深之度科技有限公司、武汉金同方科技有限公司、微脉技术有限公司、威步信息系统（上海）有限公司、天津云顶云科技有限公司、天津神州浩天科技有限公司、天津黑核科技有限公司、台达集团、台达电子企业管理（上海）有限公司、苏州同企人工智能科技有限公司、苏州汇川技术有限公司、苏州恒智友软件有限公司、视联动力信息技术股份有限公司、世邦通信股份有限公司、沈阳明致软件有限公司、神州数码集团股份有限公司、深圳市中达优控科技有限公司、深圳市圆梦云科技有限公司、深圳市一号互联科技有限公司、深圳市网旭科技有限公司、深圳市四海众联网络科技有限公司、深圳市尼高企业形象设计有限公司、深圳市美科星通信技术有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市超时代软件有限公司、深圳市必联电子有限公司、深圳市百为通达科技有限公司、深圳齐心好视通云计算有限公司、深圳科士达科技股份有限公司、上海卓卓网络科技有限公司、上海智休信息科技有限公司、上海英立视数字科技有限公司、上海赛连信息科技有限公司、上海派琪网络科技有限公司、上海灵当信息科技有限公司、上海复亚智能科技有限公司、上海泛微网络科技股份有限公司、上海大漠电子科技股份有限公司、上海车赢信息技术有限公司、上海博达数据通信有限公司、上海奥威锐网络服务有限公司、熵基科技股份有限公司、陕西凯星电子科技有限责任公司、山西时空智友科技有限公司、山东

中创软件商用中间件股份有限公司、山东运筹软件有限公司、山东医然冷链科技有限公司、山东潍微科技股份有限公司、山东欧倍尔软件科技有限责任公司、山东金钟科技集团股份有限公司、厦门亿联网络技术股份有限公司、厦门市百胜通软件技术有限公司、厦门美易通软件科技有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、千城智联（上海）网络科技有限公司、启明信息技术股份有限公司、麒麟软件有限公司、邳州天目网络科技有限公司、内蒙古奇略信息技术有限公司、南通润邦网络科技有限公司、南宁南软科技发展有限公司、美林数据技术股份有限公司、漯河市大有前途网络科技有限公司、洛阳云业信息科技有限公司、龙采科技集团有限责任公司、廊坊市极致网络科技有限公司、蓝盾信息安全技术股份有限公司、京瓷集团、京瓷（中国）商贸有限公司上海分公司、金蝶软件（中国）有限公司、江下信息科技（惠州）有限公司、江苏省广电有线信息网络股份有限公司、江苏金智教育信息股份有限公司、嘉兴想天信息科技有限公司、佳能（中国）有限公司、济宁高新技术产业开发区人民检察院、吉翁电子（深圳）有限公司、慧星软件科技有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南一唯信息科技有限公司、湖南麒麟信安科技股份有限公司、湖南匠领科技有限公司、湖南创星科技股份有限公司、湖南翱云网络科技有限公司、河北中废通网络技术有限公司、合肥金星智控科技股份有限公司、杭州中宝科技有限公司、杭州雄伟科技开发股份有限公司、杭州阔知网络科技有限公司、杭州海康威视系统技术有限公司、杭州海康威视数字技术股份有限公司、瀚高基础软件股份有限公司、海南赞赞网络科技有限公司、桂林崇胜网络科技有限公司、广州云积软件技术有限公司、广州易全信息科技有限公司、广州小橘灯信息科技有限公司、广州市时代邻里邦网络科技有限公司、广州市奥威亚电子科技有限公司、广州南方卫星导航仪器有限公司、广州烈驹电子科技有限公司、广州锦铭泰软件科技有限公司、广州安网通信技术有限公司、广西南宁领众网络科技有限公司、广东天心天思软件有限公司、广东力拓网络科技有限公司、广东堡塔安全技术有限公司、福州联讯信息科技有限公司、福建亿能达信息技术股份有限公司、东软集团股份有限公司、东华医为科技有限公司、戴尔（中国）有限公司、大连华天软件有限公司、大汉软件股份有限公司、成都索贝数码科技股份有限公司、成都成电医星数字健康软件有限公司、郴州市微设网络信息服务有限公司、畅捷通信息技术股份有限公司、餐安科技（浙江）有限公司、北京中农信达信息技术有限公司、北京中控科技发展有限公司、北京中科华博科技有限公司、北京中成科信科技发展有限公司、北京羽客阿米巴软件有限责任公司、北京用友政务软件股份有限公司、北京亿信华辰软件有限责任公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京网康科技有限公司、北京通通易联科技有限公司、北京通达信科科技有限公司、北京搜狐互联网信息服务有限公司、北京硕人时代科技股份有限公司、北京数影互联科技有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京龙软科技股份有限公司、北京灵州网络技术有限

公司、北京良精志诚科技有限责任公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京捷思锐科技股份有限公司、北京华夏大地远程教育网络服务有限公司、北京宏景世纪软件股份有限公司、北京弘文恒瑞文化传播有限公司、北京和利时集团、北京大铁科技有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、暴风集团股份有限公司、百望股份有限公司、安吉加加信息技术有限公司、安徽旭帆信息科技有限公司、zzcms、NETGEAR 和 Lexmark。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、博智安全科技股份有限公司、赛尔网络有限公司、北京华顺信安信息技术有限公司、安徽锋刃信息科技有限公司、杭州默安科技有限公司、苏州棱镜七彩信息科技有限公司、河南东方云盾信息技术有限公司、山东九域信息技术有限公司、河南灵创电子科技有限公司、山东云天安全技术有限公司、重庆都会信息科技、听潮盛世(北京)科技有限公司、北京安帝科技有限公司、成都安美勤信息技术股份有限公司、北京六方云信息技术有限公司、上海纽盾科技股份有限公司、联通数字科技有限公司、苏州亿阳值通科技发展股份有限公司、山石网科通信技术股份有限公司、郑州埃文科技、杭州美创科技有限公司、江苏易安联网络技术有限公司、广州安亿信软件科技有限公司、统信软件技术有限公司、上海谋乐网络科技有限公司、江苏金盾检测技术有限公司、北京网猿科技有限公司及其他个人白帽子向 CNVD 提交了 36292 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、奇安信网神（补天平台）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 35101 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数
斗象科技（漏洞盒子）	22421	22421
奇安信网神（补天平台）	11290	11290
三六零数字安全科技集团有限公司	1256	1256
北京神州绿盟科技有限公司	612	2
深信服科技股份有限公司	458	0

安天科技集团股份有限公司	288	0
新华三技术有限公司	270	0
北京启明星辰信息安全技术有限公司	167	0
北京数字观星科技有限公司	142	0
上海交大	134	134
西安四叶草信息技术有限公司	75	75
远江盛邦（北京）网络安全科技股份有限公司	73	73
恒安嘉新（北京）科技股份公司	71	0
中国电信集团系统集成有限责任公司	33	3
京东科技信息技术有限公司	21	15
卫士通信息产业股份有限公司	8	8
北京天融信网络安全技术有限公司	7	1
南京众智维信息科技有限公司	5	5
北京知道创宇信息技术股份有限公司	4	0
北京智游网安科技有限公司	1	1
北京山石网科信息技术有限公司	233	233
博智安全科技股份有限公司	33	33
赛尔网络有限公司	26	26
北京华顺信安信息技	20	1

术有限公司		
安徽锋刃信息科技有限公司	17	17
杭州默安科技有限公司	15	15
苏州棱镜七彩信息科技有限公司	14	14
河南东方云盾信息技术有限公司	14	14
山东九域信息技术有限公司	9	9
杭州迪普科技股份有限公司	9	0
河南灵创电子科技有限公司	8	8
山东云天安全技术有限公司	8	8
重庆都会信息科技	6	6
听潮盛世(北京)科技有限公司	5	5
北京安帝科技有限公司	4	4
成都安美勤信息技术股份有限公司	4	4
北京六方云信息技术有限公司	4	4
上海纽盾科技股份有限公司	3	3
联通数字科技有限公司	3	3
苏州亿阳值通科技发展股份有限公司	2	2
中国工商银行	2	2
山石网科通信技术股份有限公司	2	2

郑州埃文科技	1	1
杭州美创科技有限公司	1	1
江苏易安联网络技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
统信软件技术有限公司	1	1
上海谋乐网络科技有限公司	1	1
江苏金盾检测技术有限公司	1	1
北京网猿科技有限公司	1	1
CNCERT 宁夏分中心	2	2
个人	585	585
合计	38372	36292

本周漏洞按类型和厂商统计

本周，CNVD 收录了 614 个漏洞。WEB 应用 284 个，应用程序 205 个，网络设备（交换机、路由器等网络端设备）71 个，智能设备（物联网终端设备）32 个，操作系统 10 个，数据库 9 个，安全产品 3 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	284
应用程序	205
网络设备（交换机、路由器等网络端设备）	71
智能设备（物联网终端设备）	32
操作系统	10
数据库	9
安全产品	3

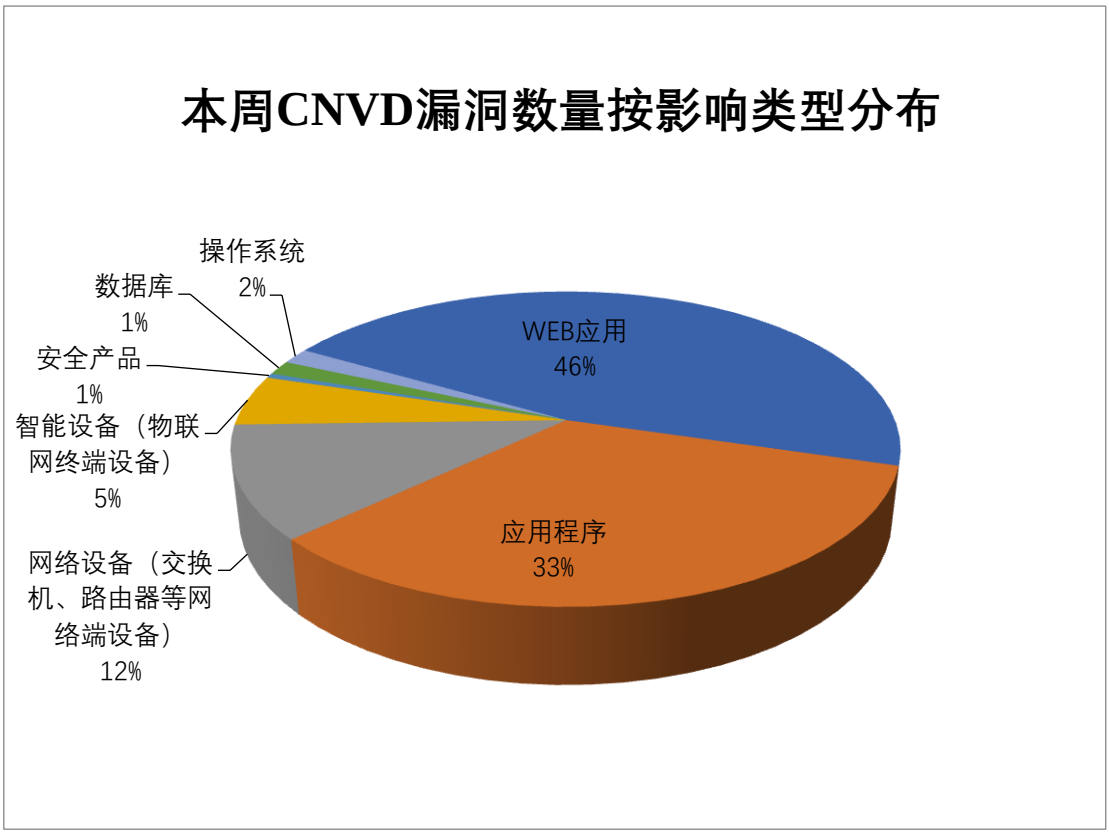

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SAP、Democritus、新华三技术有限公司等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	SAP	47	8%
2	Democritus	17	3%
3	新华三技术有限公司	12	2%
4	SIEMENS	12	2%
5	DELL	11	2%
6	Cisco	11	2%
7	Microsoft	9	1%
8	用友网络科技股份有限公司	9	1%
9	Oracle	9	1%
10	其他	477	78%

本周行业漏洞收录情况

本周，CNVD 收录了 49 个电信行业漏洞，48 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“Cisco Small Business RV Series Routers 远程代码执

行漏洞、Cisco Small Business RV Series Routers 命令注入漏洞（CNVD-2022-89251）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

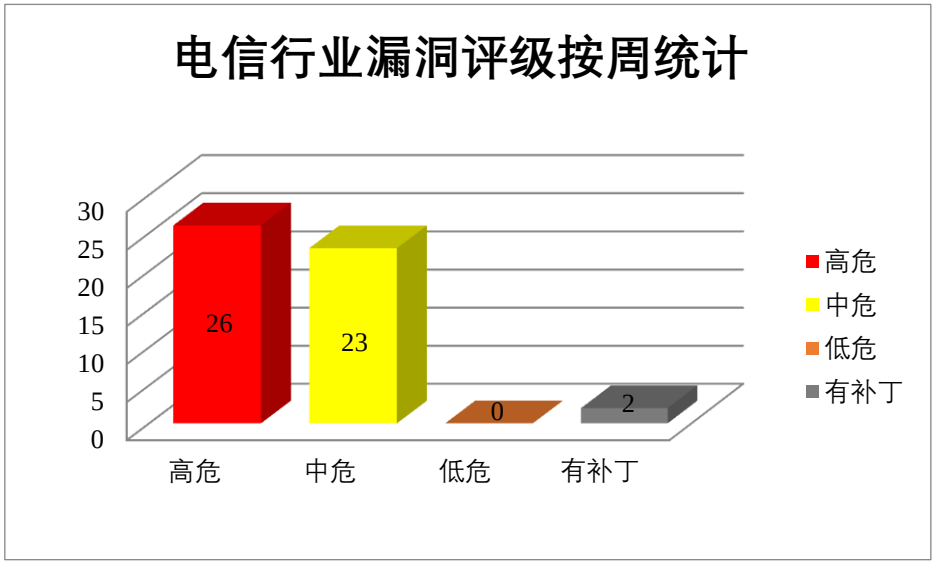

图 3 电信行业漏洞统计

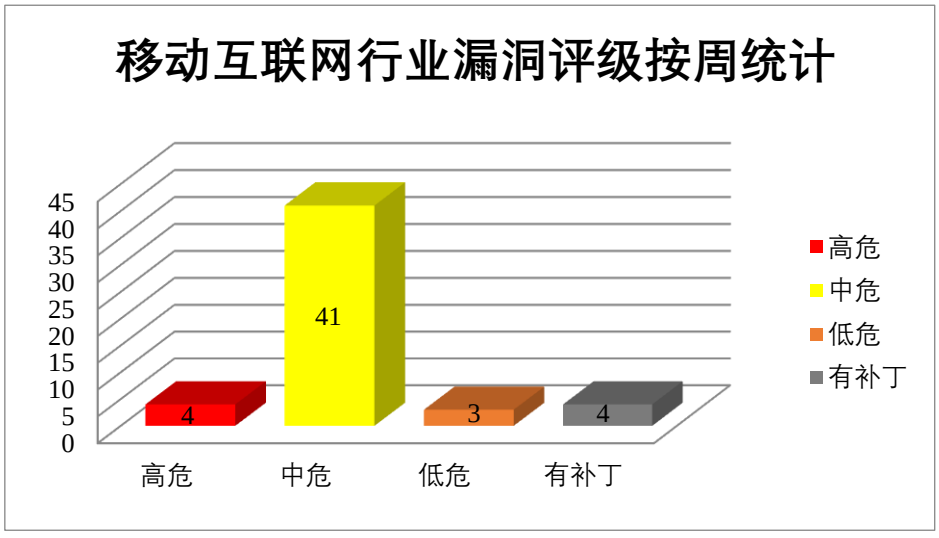

图 4 移动互联网行业漏洞统计

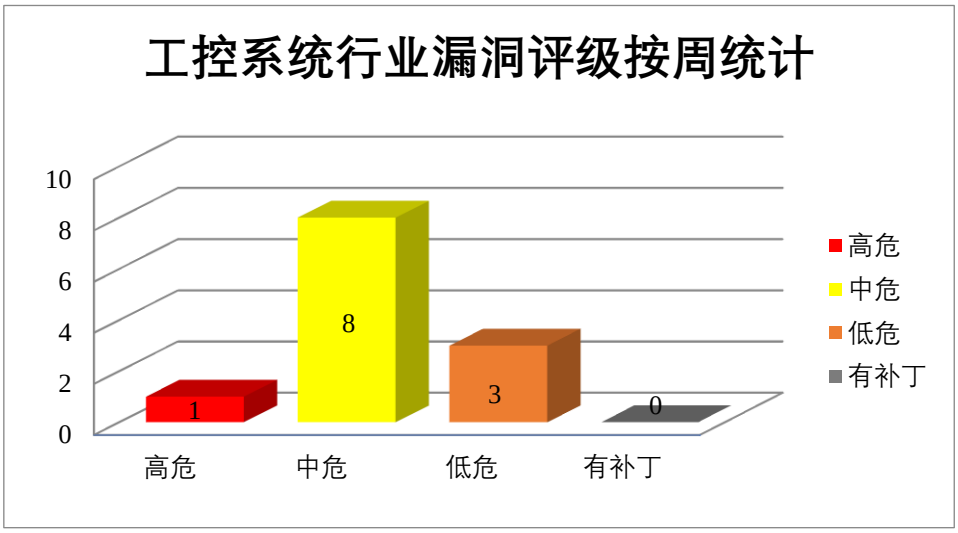

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Graphics Component 是美国微软（Microsoft）公司的图形驱动组件。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在目标主机上执行代码。

CNVD 收录的相关漏洞包括：Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2022-89421）、Microsoft Office Visio 远程代码执行漏洞（CNVD-2022-89422、CNVD-2022-89424）、Microsoft Office Graphics 远程代码执行漏洞（CNVD-2022-89423、CNVD-2022-89425、CNVD-2022-89427、CNVD-2022-89426、CNVD-2022-89428）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-89421

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89423

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89422

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89424

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89425

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89427

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89426

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89428

2、Oracle 产品安全漏洞

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞通过多种协议访问网络，从而破坏 MySQL Server，并导致 MySQL Server 挂起或频繁重复崩溃（完全 DOS）。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2022-89431、CNVD-2022-89430、CNVD-2022-89433、CNVD-2022-89432、CNVD-2022-89435、CNVD-2022-89434、CNVD-2022-89436、CNVD-2022-89437）。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-89431
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89430
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89433
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89432
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89435
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89434
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89436
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89437

3、SIEMENS 产品安全漏洞

Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。Siemens JT2GO 是一款 JT 文件查看器。本周，上述产品被披露存在多个漏洞，攻击者可利用使应用程序崩溃，从而导致拒绝服务条件，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens Teamcenter Visualization 和 JT2Go 内存错误引用漏洞、Siemens Teamcenter Visualization 和 JT2Go 越界读取漏洞（CNVD-2022-88422、CNVD-2022-88424、CNVD-2022-88426、CNVD-2022-88427、CNVD-2022-89530）、Siemens Teamcenter Visualization 和 JT2Go 文件分析漏洞（CNVD-2022-89513）、Siemens Teamcenter Visualization 和 JT2Go 越界写入漏洞。其中，除“Siemens Teamcenter Visualization 和 JT2Go 文件分析漏洞（CNVD-2022-89513）”外其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-88423
https://www.cnvd.org.cn/flaw/show/CNVD-2022-88422
https://www.cnvd.org.cn/flaw/show/CNVD-2022-88425
https://www.cnvd.org.cn/flaw/show/CNVD-2022-88424

https://www.cnvd.org.cn/flaw/show/CNVD-2022-88426

https://www.cnvd.org.cn/flaw/show/CNVD-2022-88427

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89513

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89530

4、Cisco 产品安全漏洞

Cisco Firepower Threat Defense（FTD）和 Cisco Adaptive Security Appliances Software（ASA Software）都是美国思科（Cisco）公司的产品。Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。该平台提供了对数据和网络资源的高度安全的访问等功能。Cisco RoomOS Software 和 Cisco TelePresence Collaboration Endpoint Software 都是美国思科（Cisco）公司的产品。Cisco RoomOS Software 是一套用于 Cisco 设备的自动管理软件。该软件主要用于升级、管理 Cisco 设备的主板固件。Cisco TelePresence Collaboration Endpoint Software 是一套协作终端软件。Cisco Small Business RV Series Routers 是美国思科（Cisco）公司的一款 RV 系列路由器。Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。Cisco Enterprise NFV Infrastructure Software 是美国思科（Cisco）公司的一套 NVF 基础架构软件平台。该平台可以通过中央协调器和控制器实现虚拟化服务的全生命周期管理。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成高 CPU 利用率，从而导致拒绝服务，在受影响的设备上执行任意代码等。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 和 Cisco Adaptive Security Appliances Software 拒绝服务漏洞、Cisco TelePresence Collaboration Endpoint and RoomOS Software 拒绝服务和信息泄露漏洞、Cisco Small Business RV Series Routers 远程代码执行漏洞、Cisco SD-WAN vManage Software 信息泄露漏洞（CNVD-2022-89247）、Cisco Enterprise NFV Infrastructure Software 命令注入漏洞（CNVD-2022-89248）、Cisco Enterprise NFV Infrastructure Software 权限许可和访问控制问题漏洞（CNVD-2022-89249）、Cisco Small Business RV Series Routers 命令注入漏洞（CNVD-2022-89251）、Cisco Enterprise NFV Infrastructure Software XML 外部实体注入漏洞。其中，除“Cisco Firepower Threat Defense 和 Cisco Adaptive Security Appliances Software 拒绝服务漏洞、Cisco TelePresence Collaboration Endpoint and RoomOS Software 拒绝服务和信息泄露漏洞、Cisco SD-WAN vManage Software 信息泄露漏洞（CNVD-2022-89247）、Cisco Enterprise NFV Infrastructure Software XML 外部实体注入漏洞”外其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-89243

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89245

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89246

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89247

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89248

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89249

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89251

https://www.cnvd.org.cn/flaw/show/CNVD-2022-89250

5、Aruba Networks ArubaOS 和 InstantOS 缓冲区溢出漏洞

ArubaOS 是 Aruba Mobility Controllers、Mobility Master 和控制器管理的接入点（APs）的网络操作系统。InstantOS 是一个基于 Arch Linux 的发行版。本周，Aruba Networks ArubaOS 和 InstantOS 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞在系统上执行任意代码。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-88806

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2022-88796	EyesOfNetwork 本地文件包含漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/EyesOfNetworkCommunity/eonweb/issues/120
CNVD-2022-88795	EyesOfNetwork SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/EyesOfNetworkCommunity/eonweb/issues/120
CNVD-2022-88798	mailcow 重定向漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-vjgf-cp5p-wm45
CNVD-2022-88803	Wazuh 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/wazuh/wazuh/pull/14801
CNVD-2022-88810	ToaruOS 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/klange/toaruos/commit/5d36d27bb9da768ae45dadd5a6b50c8981935d82

CNVD-2022-88811	Check Point ZoneAlarm Extreme Security 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zonealarm.com/software/extreme-security/release-history
CNVD-2022-88813	Strapi SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/strapi/strapi/releases/tag/v4.1.10
CNVD-2022-88812	Orckestra C1 CMS 反序列化漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/Orckestra/C1-CMS-Foundation/security/advisories/GHSA-gfhp-jgp6-838j
CNVD-2022-88817	Bifrost 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/brokercap/Bifrost/releases/tag/v1.8.7-release
CNVD-2022-88820	NuProcess 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/brettwooldridge/NuProcess/commit/29bc09de561bf00ff9bf77123756363a9709f868

小结：本周，Microsoft 产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在目标主机上执行代码。此外，Oracle、SIEMENS、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过多种协议访问网络，从而破坏 MySQL Server，并导致 MySQL Server 挂起或频繁重复崩溃（完全 DOS），在受影响的设备上执行任意代码等。另外，Aruba Networks ArubaOS 和 InstantOS 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞在系统上执行任意代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Advantech iView SQL 注入漏洞

验证描述

Advantech iView 是中国研华（Advantech）公司的一个基于简单网络协议（SNMP）来对 B+B SmartWorx 设备进行管理的软件。

Advantech iView 5.7.04.6469 版本存在 SQL 注入漏洞，该漏洞源于在其 ConfigurationServlet 端点中存在缺陷，攻击者可利用漏洞在 setConfiguration 操作中创建一个特殊的 column_value 参数，以绕过 com.imc.iview.utils.CUtils.checkSQLInjection()中的检查来

执行 SQL 语句，获取数据库数据。

验证信息

POC 链接：https://www.tenable.com/security/research/tra-2022-32

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-88792

信息提供者

新华三技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 黑客出售 4 亿 Twitter 用户数据库

一名用户名 Ryushi 的用户在黑客论坛 Breached 兜售 4 亿 Twitter 用户的数据库，声称是利用 Twitter API 的漏洞抓取的，包括了电子邮件、用户名、姓名、粉丝数、创建日期和电话号码。

参考链接：https://www.solidot.org/story?sid=73753

2. Raspberry Robin 恶意软件攻击电信和政府

Raspberry Robin 蠕虫攻击被发现针对拉丁美洲、澳大利亚和欧洲的电信和政府办公系统。

参考链接：https://securityaffairs.co/wordpress/139964/breaking-news/raspberry-robin-targets-telecom-governments.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537