国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 11 月 28 日-2022 年 12 月 4 日 **2022 年第 48 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 558 个，其中高危漏洞 166 个、中危漏洞 282 个、低危漏洞 110 个。漏洞平均分值为 5.74。本周收录的漏洞中，涉及 0day 漏洞 349 个（占 63%），其中互联网上出现“Hospital Management System SQL 注入漏洞（CNVD-2022-83601）、Money Transfer Management System 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 16272 个，与上周（39112 个）环比减少 58%。

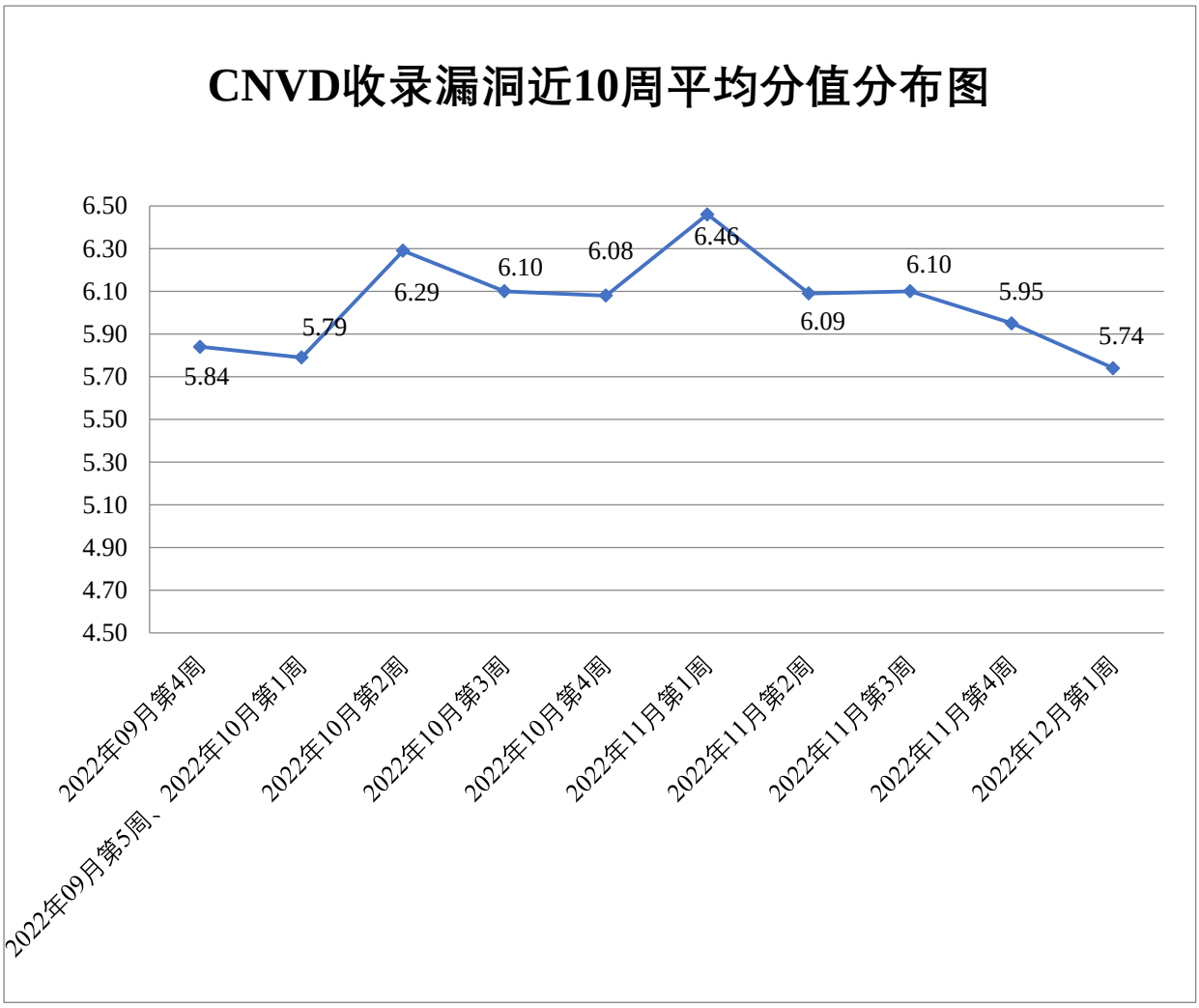

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 53 起，向基础电信企业通报漏洞事件 45 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 1492 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 367 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 222 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：

珠海新华通软件股份有限公司、重庆中联信息产业有限责任公司、众勤通信设备贸易（上海）有限公司、中山市岩峰照明科技有限公司、中健康（北京）高血压医疗科技有限公司、智互联（深圳）科技有限公司、政和科技股份有限公司、郑州鑫胜电子科技有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、长沙朗深信息技

术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、星锐蓝海网络科技有限公司、信呼、新疆云景网络科技有限公司、新都（青岛）办公系统有限公司、西安卓立科技实业有限公司、武汉众智鸿图科技有限公司、武汉天地伟业科技有限公司、五株科技股份有限公司、天地（常州）自动化股份有限公司、台达集团、苏州科达科技股份有限公司、四平市九州易通科技有限公司、水月居科技有限公司、深圳维盟科技股份有限公司、深圳市唯德科创信息有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市富士施乐实业有限公司、深圳市必联电子有限公司、深圳齐心好视通云计算有限公司、深圳飞思安诺网络技术有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海万欣计算机信息科技有限公司、上海会畅通讯股份有限公司、上海格诗网络科技有限公司、上海泛微网络科技股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山西牛之云网络科技有限公司、山东旗帜信息有限公司、若依、任子行网络技术股份有限公司、普联技术有限公司、南京云网汇联软件技术有限公司、梦想 CMS、零视技术（上海）有限公司、奎文区广文海宏软件开发中心、狂雨小说 cms、凯盛融英信息科技（上海）股份有限公司、劲旅环境科技股份有限公司、金蝶软件（中国）有限公司、江苏未至科技股份有限公司、江苏省广电有线信息网络股份有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、淮南市讯网信息技术有限公司、华夏 ERP、弘扬软件股份有限公司、河北鑫考教育科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州三汇信息工程有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、杭州博采网络科技股份有限公司、国网智能科技股份有限公司、贵州数立行科技有限公司、广州图创计算机软件开发有限公司、广州思迈特软件有限公司、广州合富科技有限公司、广州诚行网络科技股份有限公司、广东鹏为软件有限公司、构建未来（深圳）科技有限公司、大唐电信科技股份有限公司、成都生动网络科技有限公司、沧州佳蓝网络科技有限公司、北京中远麒麟科技有限公司、北京致远互联软件股份有限公司、北京映翰通网络技术股份有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京信路威科技股份有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京特夫克软件开发有限公司、北京时空智友科技有限公司、北京睿博康科技有限公司、北京派网软件有限公司、北京慕华信息科技有限公司、北京迈道科技有限公司、北京宏景世纪软件股份有限公司、北京和利时集团、北京国尚信科技有限公司、北京锋脉智软科技有限公司、北京东方通科技股份有限公司、北京百卓网络技术有限公司、北京奥信汽车服务有限公司、北大医疗信息技术有限公司、北大方正集团有限公司、阿里巴巴集团安全应急响应中心、zzzcms、ZZCMS、PHPCMS、NETGEAR、MuYuCMS、LMCMS 和 ACTi。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司、厦门服云信息科技有限公司、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、北京升鑫网络科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、贵州多彩网安科技有限公司、安徽锋刃信息科技有限公司、河南灵创电子科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、博智安全科技股份有限公司、赛尔网络有限公司、山东云天安全技术有限公司、上海齐同信息科技有限公司、山东九域信息技术有限公司、山石网科通信技术股份有限公司、河南东方云盾信息技术有限公司、华鲁数智信息技术（北京）有限公司、上海纽盾科技股份有限公司、重庆易阅科技有限公司、苏州棱镜七彩信息科技有限公司、江苏保旺达软件技术有限公司、联通沃悦读科技文化有限公司、河北千诚电子科技有限公司、山东新潮信息技术有限公司、浙江木链物联网科技有限公司、江苏网擎信息技术有限公司、北京微步在线科技有限公司、杭州海康威视数字技术股份有限公司、广东唯顶信息科技股份有限公司、中国人寿保险股份有限公司、杭州默安科技有限公司、西安交大捷普网络科技有限公司、江苏国泰新点软件有限公司及及其他个人白帽子向 CNVD 提交了 16272 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 14228 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）	12319	12319
三六零数字安全科技集团有限公司	959	959
北京启明星辰信息安全技术有限公司	721	0
奇安信网神（补天平台）	599	599
北京神州绿盟科技有限公司	450	89
上海交大	351	351
厦门服云信息科技有限公司	369	0
安天科技集团股份有限公司	321	0
新华三技术有限公司	217	0

深信服科技股份有限公司	205	5
西安四叶草信息技术有限公司	200	200
南京众智维信息科技有限公司	130	130
北京数字观星科技有限公司	104	0
恒安嘉新(北京)科技股份公司	100	0
远江盛邦（北京）网络安全科技股份有限公司	96	96
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	54	0
杭州迪普科技股份有限公司	30	2
京东科技信息技术有限公司	28	0
北京天融信网络安全技术有限公司	28	2
中国电信集团系统集成有限责任公司	26	0
北京知道创宇信息技术有限公司	26	0
北京信联科汇科技有限公司	5	5
内蒙古云科数据服务股份有限公司	3	3
北京华顺信安信息技术有限公司	500	0
北京山石网科信息技术有限公司	245	245

北京升鑫网络科技有限公司	62	62
奇安星城网络安全运营服务（长沙）有限公司	28	28
贵州多彩网安科技有限公司	27	27
安徽锋刃信息科技有限公司	23	23
河南灵创电子科技有限公司	14	14
北京云科安信科技有限公司（Seraph 安全实验室）	14	14
博智安全科技股份有限公司	13	13
赛尔网络有限公司	9	9
山东云天安全技术有限公司	9	9
上海齐同信息科技有限公司	8	8
山东九域信息技术有限公司	7	7
山石网科通信技术股份有限公司	7	7
河南东方云盾信息技术有限公司	5	5
华鲁数智信息技术（北京）有限公司	5	5
上海纽盾科技股份有限公司	4	4
重庆易阅科技有限公司	4	4
苏州棱镜七彩信息科技有限公司	2	2

江苏保旺达软件技术有限公司	2	2
联通沃悦读科技文化有限公司	2	2
河北千诚电子科技有限公司	2	2
山东新潮信息技术有限公司	1	1
浙江木链物联网科技有限公司	1	1
江苏网擎信息技术有限公司	1	1
北京微步在线科技有限公司	1	1
杭州海康威视数字技术股份有限公司	1	1
广东唯顶信息科技股份有限公司	1	1
中国人寿保险股份有限公司	1	1
杭州默安科技有限公司	1	1
西安交大捷普网络科技有限公司	1	1
江苏国泰新点软件有限公司	1	1
中国工商银行	1	1
CNCERT 贵州分中心	4	4
CNCERT 河南分中心	1	1
CNCERT 浙江分中心	1	1
个人	1003	1003
报送总计	19412	16272

本周漏洞按类型和厂商统计

本周，CNVD 收录了 558 个漏洞。WEB 应用 274 个，应用程序 164 个，网络设备（交换机、路由器等网络端设备）73 个，智能设备（物联网终端设备）23 个，安全产品 12 个，操作系统 11 个，数据库 1 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	274
应用程序	164
网络设备（交换机、路由器等网络端设备）	73
智能设备（物联网终端设备）	23
安全产品	12
操作系统	11
数据库	1

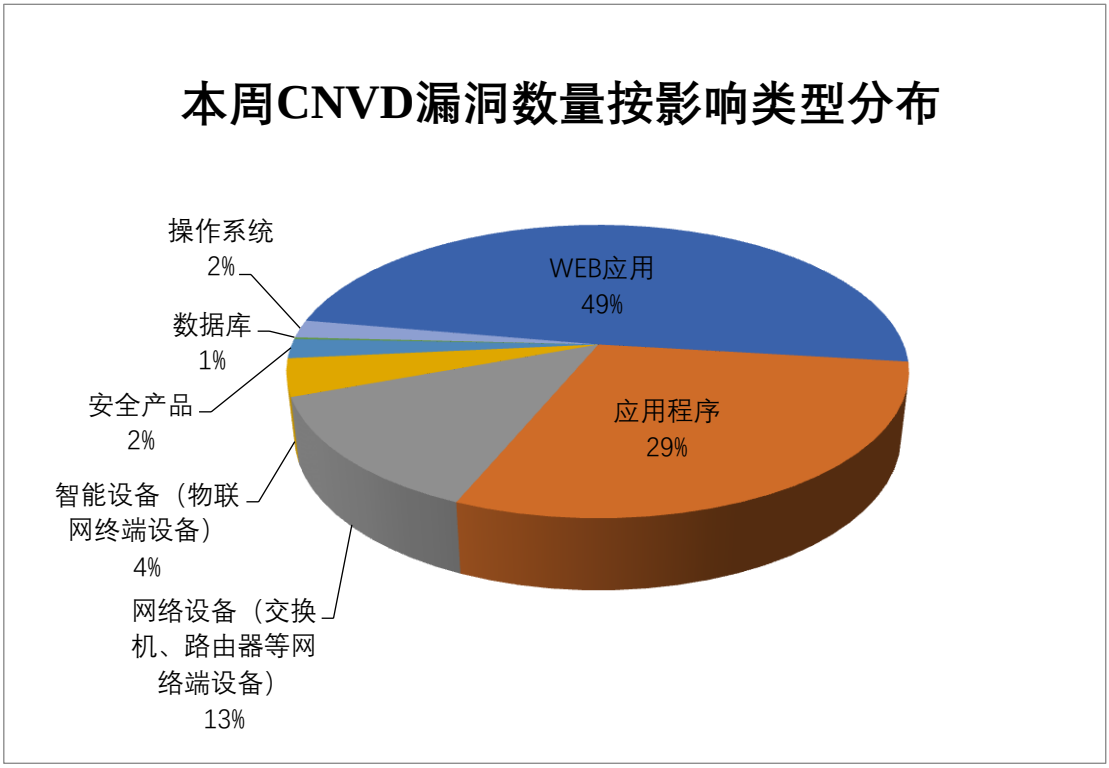

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Microsoft、杭州冠航科技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	WordPress	50	9%
2	Microsoft	14	3%
3	杭州冠航科技有限公司	14	3%
4	Apache	14	3%

5	杭州短趣网络传媒技术有限公司	13	2%
6	Tuxera	12	2%
7	IBM	12	2%
8	Jenkins	11	2%
9	用友网络科技股份有限公司	11	2%
10	其他	407	72%

本周行业漏洞收录情况

本周，CNVD 收录了 39 个电信行业漏洞，26 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“TCL LinkHub Mesh Wi-Fi confctl_set_guest_wlan 拒绝服务漏洞、TCL LinkHub Mesh Wi-Fi 缓冲区溢出漏洞”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/

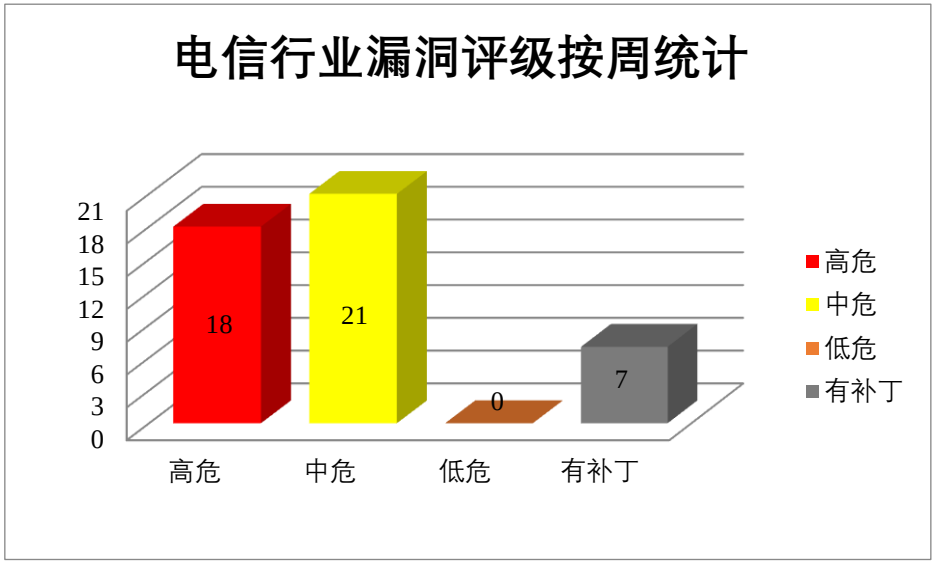

图 3 电信行业漏洞统计

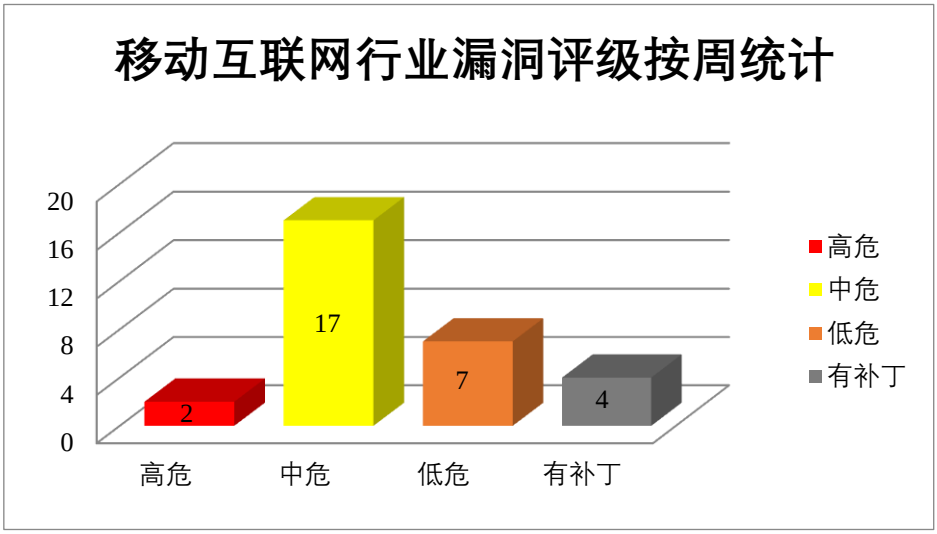

图 4 移动互联网行业漏洞统计

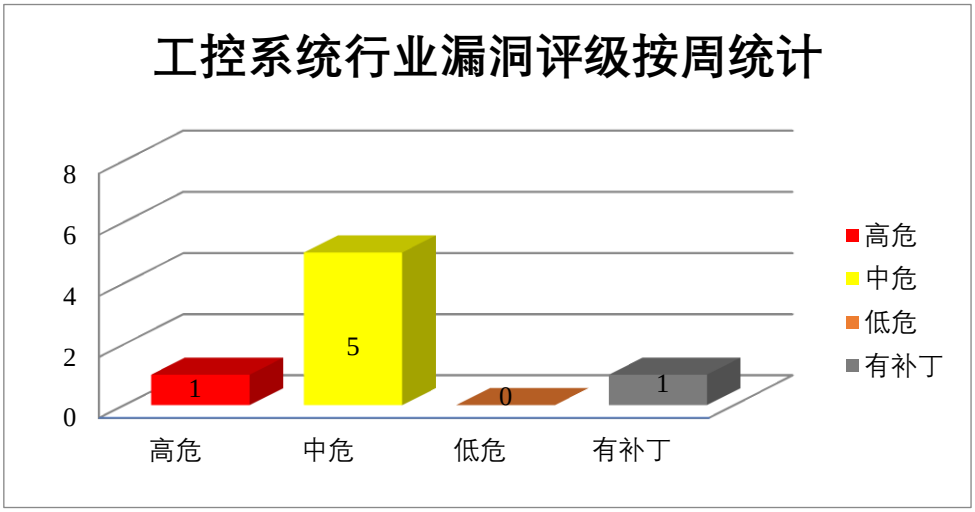

图 5 工控系统行业漏洞统计

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、 Dell 产品安全漏洞

Dell SupportAssist for Business PCs 是一款适用于企业电脑的客户端应用程序。该程序提供自动化、主动和预测性技术进行故障排除等。Dell SupportAssist for Home PCs 是一款适用于家庭电脑的客户端应用程序。该程序提供自动化、主动和预测性技术进行故障排除等。Dell SupportAssist Client 是美国戴尔（DELL）公司的一款客户端应用程序。该程序提供自动化、主动和预测性技术进行故障排除等。Dell PowerStore 全闪存数据存储设备采用以数据为中心、具有高度适应性的智能基础架构来提供 AppsON 功能，实现传统和现代工作负载的转型。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取对系统的管理员访问权限，导致信息泄露和任意执行代码等。

CNVD 收录的相关漏洞包括：Dell SupportAssist for Home PCs and Dell Support Assist for Business PCs 代码问题漏洞、Dell SupportAssist Client 代码问题漏洞、Dell SupportAssist Client Consumer and Dell SupportAssist Client Commercial 代码问题漏洞、Dell PowerStore 开放端口漏洞、Dell PowerStore 资源管理错误漏洞、Dell PowerStore 授权问题漏洞、Dell PowerStore 公式注入漏洞、Dell PowerStore 操作系统命令注入漏洞。其中，除“Dell SupportAssist Client 代码问题漏洞、Dell PowerStore 公式注入漏洞”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-2022-83203

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83202

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83201

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83204

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83209

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83208

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83206

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83205

2、IBM 产品安全漏洞

IBM Rational ClearCase 是美国 IBM 公司的一套软件配置管理解决方案。该方案可提供版本控制、工作空间管理、并行开发支持和构建审计等功能。IBM AIX 是美国国际商业机器（IBM）公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。 IBM CICS TX 是美国国际商业机器（IBM）公司的一个综合的、单一的事务运行时包。IBM DataPower Gateway 是美国 IBM 公司的一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台。该平台可利用专用网关平台跨渠道保护、集成和优化访问。IBM WebSphere Application Server（WAS）是美国国际商业机器（IBM）公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。 IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取密码及文档数据库的未授权访问权限，在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期的功能，导致受信任会话中的凭据泄露等。

CNVD 收录的相关漏洞包括： IBM Rational ClearCase GIT connector 信任管理问题漏洞、IBM AIX 命令注入漏洞、IBM CICS TX 加密问题漏洞（CNVD-2022-83579、CNVD-2022-83580）、IBM DataPower Gateway 跨站点请求伪造漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2022-83582）、IBM QRadar SIEM 信息泄

露漏洞（CNVD-2022-83586）、IBM QRadar SIEM 访问控制错误漏洞（CNVD-2022-83584）。其中，“IBM CICS TX 加密问题漏洞（CNVD-2022-83579、CNVD-2022-83580）、IBM DataPower Gateway 跨站点请求伪造漏洞、IBM QRadar SIEM 访问控制错误漏洞（CNVD-2022-83584）”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-2022-82253
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83581
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83580
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83579
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83583
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83582
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83586
https://www.cnvd.org.cn/flaw/show/CNVD-2022-83584

3、 Apache 产品安全漏洞

Apache Hama 是美国阿帕奇（Apache）公司的一个基于批量同步并行计算技术的分布式计算框架。用于大规模科学计算，例如矩阵，图形和网络算法。Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。Apache Heron 是一款分布式、具有容错功能的实时流处理引擎。Apache Pulsar 是美国阿帕奇（Apache）基金会的一个用于云环境种，集消息、存储、轻量化函数式计算为一体的分布式消息流平台。该软件支持多租户、持久化存储、多机房跨区域数据复制，具有强一致性、高吞吐以及低延时的高可扩展流数据存储特性。Apache JSPWiki 是美国阿帕奇（Apache）基金会的一款基于 Java、Servlet 和 JSP 构建的开源 WikiWiki 引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过路径遍历导致信息泄露，在任务执行上下文中执行的命令，而无需对 DAG 文件进行写入访问等。

CNVD 收录的相关漏洞包括：Apache Hama 路径遍历漏洞、Apache Airflow 操作系统命令注入漏洞（CNVD-2022-83588、CNVD-2022-83589）、Apache Heron 注入漏洞、Apache Pulsar 信任管理问题漏洞（CNVD-2022-83591）、Apache JSPWiki 跨站脚本漏洞（CNVD-2022-83597、CNVD-2022-83598、CNVD-2022-83599）。其中，“Apache Hama 路径遍历漏洞、Apache Airflow 操作系统命令注入漏洞（CNVD-2022-83589）、Apache Heron 注入漏洞、Apache Pulsar 信任管理问题漏洞（CNVD-2022-83591）”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-2022-83590

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83589

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83588

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83592

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83591

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83597

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83598

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83599

4、Microsoft 产品安全漏洞

Microsoft Azure Site Recovery 是美国微软（Microsoft）公司的一种站点恢复 (DR aaS)，用于云和混合云架构。Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Azure Site Recovery 权限提升漏洞（CNVD-2022-84109、CNVD-2022-84111）、Microsoft Azure Site Recovery 远程代码执行漏洞（CNVD-2022-84112）、Microsoft Windows DNS Server 远程代码执行漏洞（CNVD-2022-84113、CNVD-2022-84114、CNVD-2022-84115、CNVD-2022-84116、CNVD-2022-84117）。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-2022-84109

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84111

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84112

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84113

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84114

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84115

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84116

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84117

5、TCL LinkHub Mesh Wi-Fi 操作系统命令注入漏洞

TCL LinkHub Mesh Wi-Fi 是 TCL 公司的一款路由器。本周，TCL LinkHub Mesh Wi-Fi 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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-2022-82016

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-2022-82013	TCL LinkHub Mesh Wi-Fi ucloud_set_node_location 功能堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://mobile-support.tcl.com/global/en/service-support-router/linkhub-mesh-wifi-ms1g.html
CNVD-2022-82015	TCL LinkHub Mesh Wi-Fi 信息泄露漏洞	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.tcl.com/us/en/products/connected-home/linkhub/linkhub-mesh-wifi-system-3-pack
CNVD-2022-82014	TCL LinkHub Mesh Wi-Fi ucloud_del_node 功能拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.tcl.com/us/en/products/connected-home/linkhub/linkhub-mesh-wifi-system-3-pack
CNVD-2022-82017	TCL LinkHub Mesh Wi-Fi confctl_set_master_wlan 功能拒绝服务漏洞	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.tcl.com/us/en/products/connected-home/linkhub/linkhub-mesh-wifi-system-3-pack
CNVD-2022-82019	Online Reviewer System 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcecodester.com/php/12937/online-reviewer-system-using-phppdo.html
CNVD-2022-82021	TCL LinkHub Mesh Wi-Fi confctl_get_master_wlan 功能信息泄露漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://mobile-support.tcl.com/global/en/service-support-router/linkhub-mesh-wifi-ms1g.html
CNVD-2022-82262	Wordpress Plugin Paid Memberships Pro SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/6c25a5f0-a137-4ea5-9422-8ae393d7b76b
CNVD-2022-82263	Wordpress Plugin Paid Memberships Pro SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/6c25a5f0-a137-4ea5-9422-8ae393d7b76b
CNVD-2022-82572	Synology Calendar 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/advisory/Synology_SA_20_07

CNVD-2022-82573	Synology Media Server 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/advisory/Synology_SA_20_24

小结：本周，Dell 产品被披露存在多个漏洞，攻击者可利用漏洞获取对系统的管理员访问权限，导致信息泄露和任意执行代码。此外，IBM、Apache、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取密码及文档数据库的未授权访问权限，在任务执行上下文中执行的命令，而无需对 DAG 文件进行写入访问等。另外，TCL LinkHub Mesh Wi-Fi 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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、Hospital Management System SQL 注入漏洞（CNVD-2022-83601）

验证描述

Hospital Management System 是一款医院管理系统。包含病患信息管理、预约服务、财务管理等模块。

Hospital Management System v1.0 版本中存在 SQL 注入漏洞。该漏洞源于 admin.php 中的 adminname 参数缺少有效验证有关。攻击者可利用该漏洞对目标有针对性的发起 SQL 注入攻击，危害站点系统安全。

验证信息

POC 链接：https://github.com/HH1F/Hospital-Management-System-V1.0-SQLi

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-83601

信息提供者

杭州迪普科技股份有限公司

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. 三星小米等厂商均受影响，谷歌披露威胁安卓设备的高危漏洞

12 月 3 日消息，谷歌安卓合作伙伴漏洞计划（APVI）网站上的一个新帖子中，曝光了一个影响安卓设备的安全漏洞。黑客利用该漏洞，就能够在三星、LG、小米等诸多 OEM 厂商品牌手机中植入恶意软件。而且这些恶意软件可以获得系统级别的最高权限。

参考链接：https://www.ithome.com/0/658/513.htm

2. 俄罗斯政府机构遭 CryWiper 勒索软件攻击

外媒报道称，俄罗斯市长的办公室和法院遭到了一种新的加密病毒的攻击。该程序在计算机上对数据进行编码，要求支付赎金——超过 50 万卢布。但是，即使您将这笔金额转移给黑客，病毒也会将文件完全删除。

参考链接：https://www.securitylab.ru/news/535064.php

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