国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 05 月 09 日-2022 年 05 月 15 日 **2022 年第 19 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 178 个，其中高危漏洞 67 个、中危漏洞 92 个、低危漏洞 19 个。漏洞平均分值为 5.88。本周收录的漏洞中，涉及 0day 漏洞 86 个（占 48%），其中互联网上出现“WUZHI CMS SQL 注入漏洞（CNVD-2022-36985）、Bludit CMS 跨站脚本漏洞”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 8445 个，与上周（14613 个）环比减少 42%。

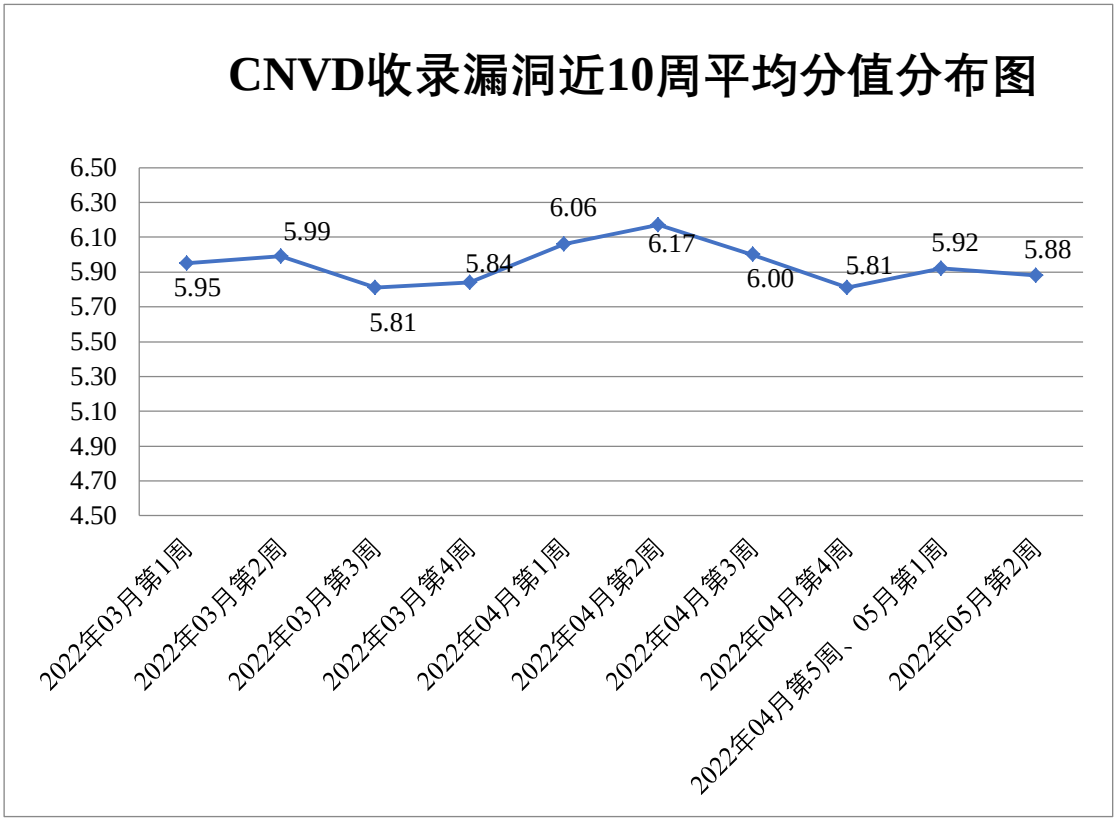

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 44 起，向基础电信企业通报漏洞事件 43 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 516 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 90 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 128 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、浙江中易慧能科技有限公司、浙江浙大中控信息技术有限公司、浙江大华技术股份有限公司、云南博尔科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新道科技股份有限公司、夏普商贸（中国）有限公司、西安中望软件资讯有限责任公司、西安瑞友信息技术资讯有限公司、武汉众为信息技术有限公司、微软（中国）有限公司、网经科技（苏州）有限公司、通赢天下（天津）网络科技有限公司、四川万博教育软件股份有限公司、神州数码控股有限公司、深圳维盟科技股份有限公司、深圳市镇安科技有限公司、深圳市思迪信息技术股份有限公司、深圳市库迪科技有限公司、深圳市集时通讯有限公司、深圳市吉祥腾达科技有限公司、深圳市河辰通讯技术有限公司、深圳市和为顺网络技术有限公司、深圳市共济科技股份有限公司、深圳市多酷科技有限公司、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、深圳科士达科技股份有限公司、上海展盟网络科技有限公司、上海云翌通信科技有限公司、上海焱凤信息技术有限公司、上海携宁计算机科技股份有限公司、上海威派格智慧水务股份有限公司、上海树维信息科技有限公司、上海商汤智能科技有限公司、上海商派网络科技有限公司、上海华测导航技术股份有限公司、上海博达数据通信有限公司、上海爱数信息技术股份有限公司、上海艾泰科技有限公司、山东欧倍尔软件科技有限责任公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、全天数据管理有限公司、麒麟软件有限公司、普联技术有限公司、品道电子商务有限公司、内蒙古奔富畜牧业发展有限公司、南京天溯自动化控制系统有限公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、蓝盾信息安全技术股份有限公司、昆明云涛科技有限公司、京瓷办公信息系统（中国）有限公司、金满坝（深圳）科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、湖南建研信息技术股份有限公司、恒锋信息科技股份有限公司、杭州三汇信息工程有限公司、杭州企盼信息科技有限公司、杭州吉拉科技有限公司、杭州宏服软件有限公司、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、哈尔滨新中新电子股份有限公司、广州中望龙腾软件股份有限公司、广州市保伦电子有限公司、广州齐博网络科技有限公司、广

州南方卫星导航仪器有限公司、广州国微软件科技有限公司、广西南宁领众网络科技有限公司、广东堡塔安全技术有限公司、福州青格软件有限公司、鼎捷软件股份有限公司、成都星锐蓝海网络科技有限公司、成都万江港利科技有限公司、成都索贝数码科技股份有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京云中融信网络科技有限公司、北京星网锐捷网络技术有限公司、北京通达信科科技有限公司、北京淘友天下科技发展有限公司、北京拓尔思信息技术股份有限公司、北京数影互联科技有限公司、北京清元优软科技有限公司、北京派网软件有限公司、北京九思协同软件有限公司、北京华远达智联科技集团有限公司、北京华宇信息技术有限公司、北京函云数据科技有限公司、北京博海琪林科技有限公司、北京百卓网络技术有限公司、安徽旭帆信息科技有限公司、安徽蓝盾光电子股份有限公司、腾讯安全应急响应中心、站帮主 CMS、勾股 CMS、Victor CMS、TRENDnet、LuckyFrame、LG、FTCMS、EZB Systems, Inc、Dreambox Visual Communications、Cisco、canonical 和 Axis Communications AB。

本周，CNVD 发布了《Microsoft 发布 2022 年 5 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7681

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、新华三技术有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。重庆都会信息科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、快页信息技术有限公司、华鲁数智信息技术（北京）有限公司、广州百蕴启辰科技有限公司、上海纽盾科技股份有限公司、山石网科通信技术股份有限公司、武汉安域信息安全技术有限公司、贵州泰若数字科技有限公司、河南信安世纪科技有限公司、山东云天安全技术有限公司、北京冠程科技有限公司、智网安云（武汉）信息技术有限公司、智网安云（武汉）信息技术有限公司、巨鹏信息科技有限公司、上海观安信息技术股份有限公司、北京国测信安科技有限公司、北京山石网科信息技术有限公司、广东蓝爵网络安全技术股份有限公司、安徽长泰科技有限公司、北京机沃科技有限公司、杭州默安科技有限公司及其他个人白帽子向 CNVD 提交了 8445 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）、上海交大、奇安信网神（补天平台）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 6153 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）	3496	3496

奇安信网神（补天平台）	1637	1637
三六零数字安全科技集团有限公司	747	747
阿里云计算有限公司	742	0
新华三技术有限公司	506	0
深信服科技股份有限公司	375	0
上海交大	273	273
杭州安恒信息技术股份有限公司	263	14
安天科技集团股份有限公司	213	0
北京神州绿盟科技有限公司	160	0
远江盛邦（北京）网络安全科技股份有限公司	157	157
北京数字观星科技有限公司	153	0
北京天融信网络安全技术有限公司	146	7
厦门服云信息科技有限公司	99	0
恒安嘉新（北京）科技股份公司	94	0
京东科技信息技术有限公司	78	0
内蒙古云科数据服务股份有限公司	74	74
北京启明星辰信息安全技术有限公司	65	3
天津市国瑞数码安全系统股份有限公司	59	0
西安四叶草信息技术	37	37

有限公司		
北京知道创宇信息技术有限公司	34	3
中国电信集团系统集成有限责任公司	19	0
南京众智维信息科技有限公司	14	14
卫士通信息产业股份有限公司	12	2
南京联成科技发展股份有限公司	12	12
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华顺信安科技有限公司	186	0
重庆都会信息科技有限公司	52	52
西门子（中国）有限公司	32	0
亚信科技（成都）有限公司	15	0
北京云科安信科技有限公司（Seraph 安全实验室）	15	15
快页信息技术有限公司	15	15
华鲁数智信息技术（北京）有限公司	15	15
广州百蕴启辰科技有限公司	14	14
上海纽盾科技股份有限公司	12	12
山石网科通信技术股份有限公司	8	8

武汉安域信息安全技术有限公司	7	7
贵州泰若数字科技有限公司	7	7
河南信安世纪科技有限公司	6	6
山东云天安全技术有限公司	3	3
北京冠程科技有限公司	3	3
智网安云（武汉）信息技术有限公司	3	3
智网安云（武汉）信息技术有限公司	2	2
巨鹏信息科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
北京国测信安科技有限公司	1	1
北京山石网科信息技术有限公司	1	1
广东蓝爵网络安全技术股份有限公司	1	1
安徽长泰科技有限公司	1	1
北京机沃科技有限公司	1	1
杭州默安科技有限公司	1	1
CNCERT 四川分中心	5	5
CNCERT 贵州分中心	1	1
个人	1790	1790
报送总计	11667	8445

本周漏洞按类型和厂商统计

本周，CNVD 收录了 178 个漏洞。WEB 应用 66 个，应用程序 56 个，网络设备（交换机、路由器等网络端设备）30 个，数据库 11 个，操作系统 9 个，智能设备（物联网终端设备）5 个，安全产品 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	66
应用程序	56
网络设备（交换机、路由器等网络端设备）	30
数据库	11
操作系统	9
智能设备（物联网终端设备）	5
安全产品	1

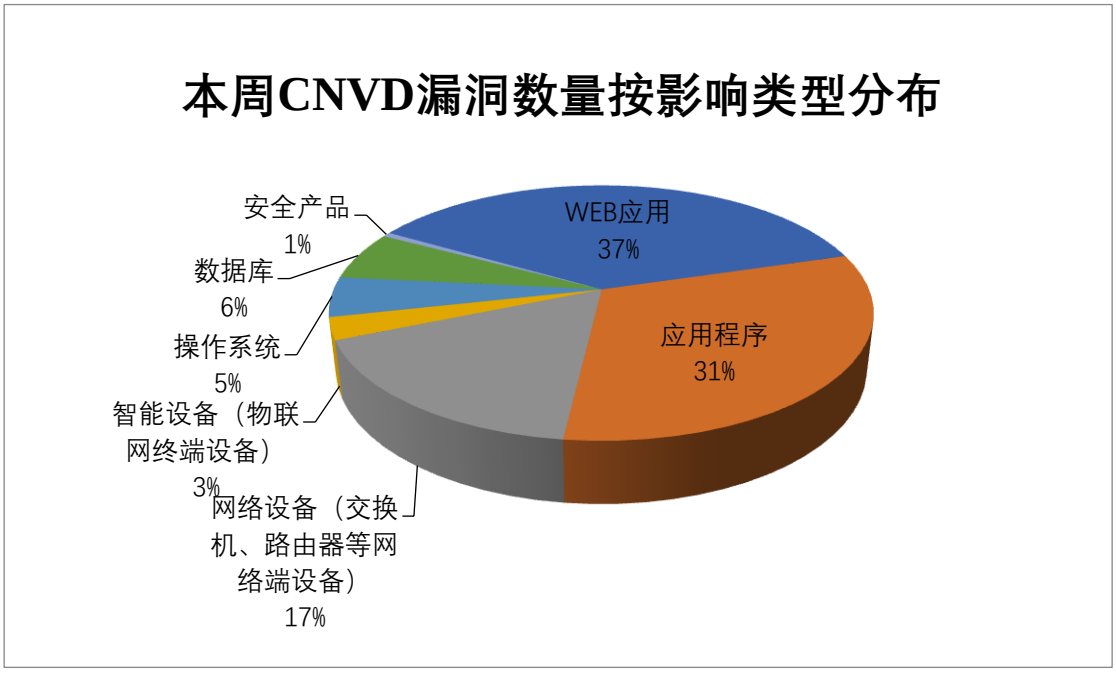

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、杭州益仕行信息技术有限公司、Oracle 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	Siemens	25	14%
2	杭州益仕行信息技术有限公司	13	7%

3	Oracle	13	7%
4	Delta Electronics	11	6%
5	IBM	9	5%
6	Mozilla	8	5%
7	北京百卓网络技术有限公司	6	3%
8	Microsoft	6	3%
9	WordPress	4	3%
10	其他	83	47%

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，2 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Siemens SIMATIC CP 44x-1 RNA 拒绝服务漏洞、Google Android 内存错误引用漏洞（CNVD-2022-36961）”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/

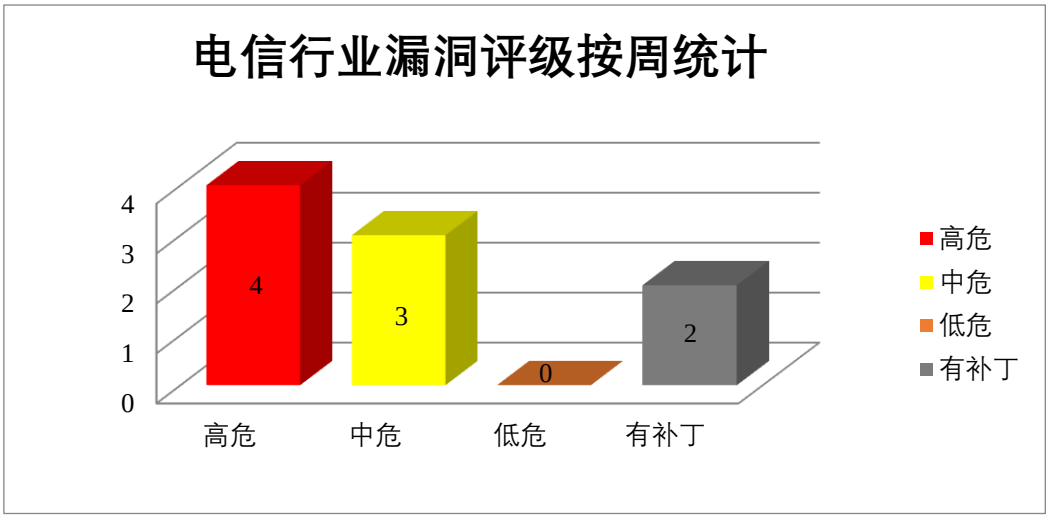

图 3 电信行业漏洞统计

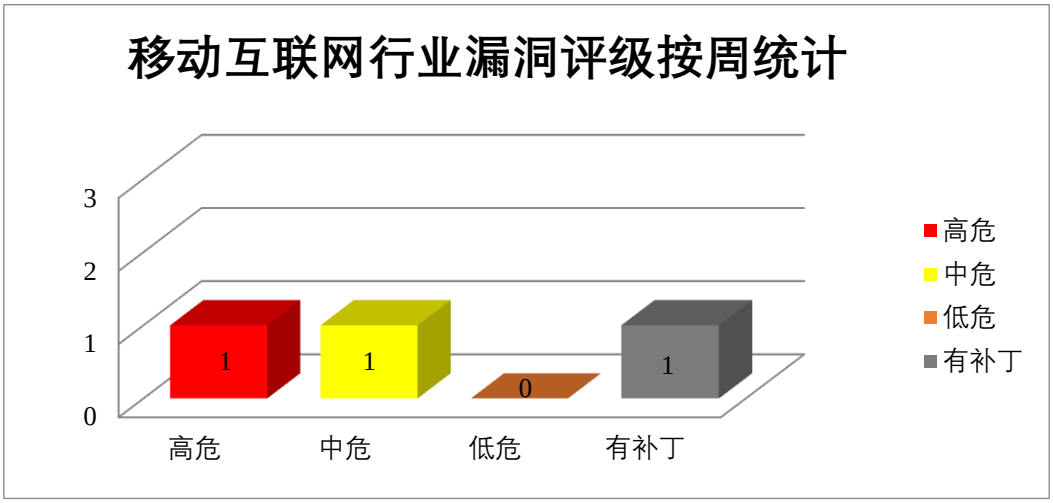

图 4 移动互联网行业漏洞统计

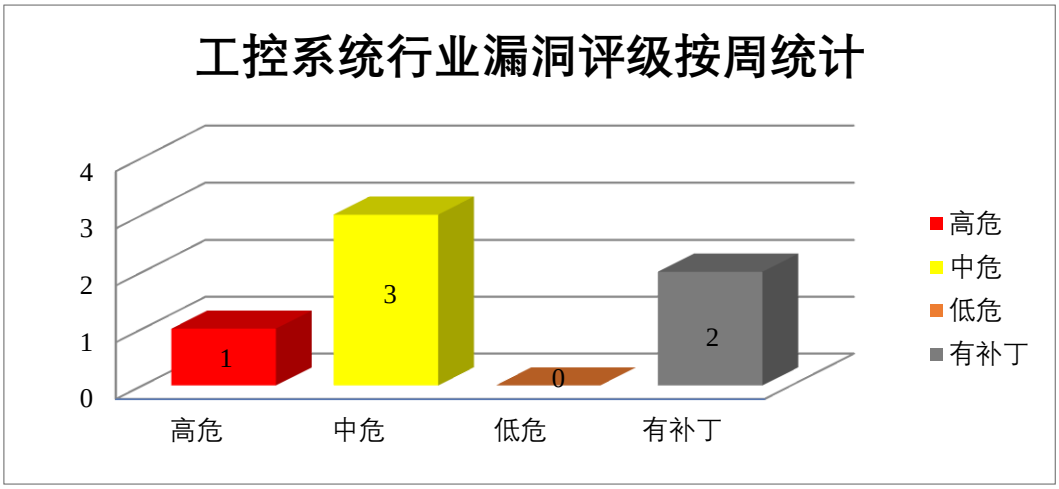

图 5 工控系统行业漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Thunderbird 是美国 Mozilla 基金会的一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。该软件支持 IMAP、POP 邮件协议以及 HTML 邮件格式。Mozilla Firefox 是一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，导致内存损坏等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 跨站脚本漏洞（CNVD-2022-36976）、Mozilla Firefox 欺骗攻击漏洞、Mozilla Firefox 无限循环漏洞、Mozilla Firefox 资源管理错误漏洞（CNVD-2022-36980）、Mozilla Firefox 安全特征问题漏洞、Mozilla Firefox MessageTask 资源管理错误漏洞、Mozilla Thunderbird 信息泄露漏洞（CNVD-2022-36982）、Mozilla Firefox 信息泄露漏洞（CNVD-2022-36981）。其中，“Mozilla Firefox 安全特征问题漏洞”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-2022-36976

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36978

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36977

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36980

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36979

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36983

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36982

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36981

2、IBM 产品安全漏洞

IBM Robotic Process Automation 是美国 IBM 公司的一种机器人流程自动化产品。IBM Cloud Pak System 是美国 IBM 公司的一套具有可配置、预集成软件的全栈、融合基础架构。IBM Robotic Process Automation 是美国 IBM 公司的一种机器人流程自动化产品。IBM Security Guardium Data Encryption 是美国 IBM 公司的一个应用软件。IBM MQ Appliance 是美国 IBM 公司的一款用于快速部署企业级消息中间件的一体机设备。IBM Watson Query 是美国 IBM 公司的一个通用查询引擎。IBM Cloud Pak for Business Automation 是美国国际商业机器公司（IBM）的一组模块化的集成软件组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞解密敏感信息，枚举账户凭证，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Robotic Process Automation 授权问题漏洞、IBM Cloud Pak System 加密问题漏洞、IBM Robotic Process Automation 信息泄露漏洞、IBM Guardium Data Encryption（GDE）跨站脚本漏洞、IBM MQ Appliance 信息泄露漏洞（CNVD-2022-36975）、IBM MQ Appliance 拒绝服务漏洞（CNVD-2022-36974）、IBM Watson Query with Cloud Pak for Data as a Service 权限提升漏洞、IBM Cloud Pak for Business Automation 访问控制错误漏洞。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-2022-36971

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36969

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36968

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36967

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36975

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36974

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36973

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36972

3、SIEMENS 产品安全漏洞

Siemens Jt2go 是一款 JT 文件查看器。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。Desigo PXC4 楼宇自动化控制器是为暖通空调系统控制而设计的。它是一款紧凑型设备，内置 IOs，能够通过额外的 TX-IO 模块扩展到您的需要。Desigo PXC5 是一款可自由编程控制器，用于 BACnet 系统级功能，如报警路由、系统范围的调度和趋势分析，以及设备监控。Desigo DXR2 控制器是可编程的自动化站，以支持终端 HVAC 设备和 TRA（全房间自动化）应用的标准控制需求。Desigo PXC3 系列自动化站可用于功能性和灵活性要求更高的建筑。SICAM P850 多功能测量装置用于采集、可视化、评估和传输电气测量变量，如交流电、交流电压、频率、功率、谐波等。SICAM P855 多功能设备用于收集、显示和传输测量的电气变量，如交流电流、交流电压、功率类型、谐波等。根据电能质量标准 IEC 61000-4-30 收集和处理测量值和事件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问设备的管理界面，在当前进程的上下文中执行代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens JT2Go 和 Teamcenter Visualization 双重释放漏洞（CNVD-2022-36381）、Siemens JT2Go 和 Teamcenter Visualization 文件解析漏洞、Siemens Desigo PXC 和 DXR Devices 远程代码执行漏洞、Siemens Desigo PXC 和 DXR Devices 不受控制资源消耗漏洞、Siemens SICAM P850 和 SICAM P855 Devices 跨站脚本漏洞（CNVD-2022-36389、CNVD-2022-36395、CNVD-2022-36391）、Siemens SICAM P850 和 SICAM P855 Devices 绕过身份验证漏洞。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-2022-36381
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36380
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36379
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36378
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36389
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36393
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36391
https://www.cnvd.org.cn/flaw/show/CNVD-2022-36395

4、Oracle 产品安全漏洞

Oracle Solaris 是美国甲骨文（Oracle）公司的一套 UNIX 操作系统。Oracle WebLogic Server 是一款适用于云环境和传统环境的应用服务中间件。Oracle MySQL 是一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。MySQL Connectors 是其中的一个连接使用 MySQL 的应用程序的驱动程序。Oracle Database Server 是一套关系数据库管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取和操作数据，执行任意代码等。

CNVD 收录的相关漏洞包括：Oracle Solaris 输入验证错误漏洞（CNVD-2022-36946）、Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-36951）、Oracle MySQL InnoDB 组件拒绝服务漏洞、Oracle Database Server 输入验证错误漏洞（CNVD-2022-36954、CNVD-2022-36953、CNVD-2022-36952、CNVD-2022-36958）、Oracle MySQL 输入验证错误漏洞（CNVD-2022-36955）。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-2022-36946

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36951

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36949

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36954

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36953

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36952

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36958

https://www.cnvd.org.cn/flaw/show/CNVD-2022-36955

5、Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-36031）

Delta Electronics DIAEnergie 是一个工业能源管理系统，用于实时监控和分析能源消耗、计算能源消耗和负载特性、优化设备性能、改进生产流程并最大限度地提高能源效率。本周，Delta Electronics DIAEnergie 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞注入任意 SQL 查询、检索和修改数据库内容以及执行系统命令。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-2022-36031

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-2022-36026	Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-36026）	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.deltaww.com/en/customerService
CNVD-2022-36030	Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-36030）	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.deltaww.com/en/customerService
CNVD-2022-36037	Dell Wyse Management Suite 文件上传漏洞	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.dell.com/support/kbdoc/000195918

CNVD-2022-36042	Dell Vnx2 Oe For File 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/kbdoc/en-us/000191155/dsa-2021-164-dell-vnx2-control-station-security-update-for-multiple-vulnerabilities
CNVD-2022-36040	Laravel 远程代码执行漏洞	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/guoyanan1g/Laravel-vul/issues/2#issue-1045655892
CNVD-2022-36387	Siemens SIMATIC WinCC Kiosk Mode 不正确初始化漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-363107.html
CNVD-2022-36396	Siemens SICAM P850 和 SICAM P855 Devices 敏感信息明文传输漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-165073.html
CNVD-2022-36399	Siemens Simcenter Femap 文件解析漏洞（CNVD-2022-36399）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-162616.html
CNVD-2022-36664	Microsoft Windows Active Directory 权限提升漏洞（CNVD-2022-36664）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923
CNVD-2022-36989	WordPress plugin RRatingg 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://wpscan.com/vulnerability/e7fe8218-4ef5-4ef9-9850-8567c207e8e6

小结：本周，Mozilla 产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，导致内存损坏等。此外，IBM、Siemens、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取和操作数据，在当前进程的上下文中执行代码，造成拒绝服务等。另外，Delta Electronics DIAEnergie 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞注入任意 SQL 查询、检索和修改数据库内容以及执行系统命令。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、Bludit CMS 跨站脚本漏洞

验证描述

Bludit CMS 是一套开源的轻量级博客内容管理系统（CMS）。

Bludit CMS v3.13.1 版本存在跨站脚本漏洞，该漏洞源于/admin/new-content 页面缺少对于用户输入数据的过滤和验证。攻击者可利用该漏洞在客户端执行 JavaScript 代码。

验证信息

POC 链接：https://github.com/joinia/webray.com.cn/blob/main/Bludit/Bluditreadme.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-36994

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. Zyxel 发布针对关键防火墙操作系统命令注入漏洞的补丁

Zyxel 已着手解决影响 Zyxel 防火墙设备的安全漏洞，该漏洞使未经身份验证的远程攻击者能够获得任意代码执行。

参考链接：https://thehackernews.com/2022/05/zyxel-releases-patch-for-critical.html

2. 惠普修复了影响 200 多种型号的固件 BUG

惠普近期发布了 BIOS 更新，修复了两个影响广泛 PC 和笔记本电脑产品的漏洞，这些漏洞允许代码以内核权限运行。

参考链接：https://www.bleepingcomputer.com/news/security/hp-fixes-bug-letting-attackers-overwrite-firmware-in-over-200-models/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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