

## 信息安全漏洞周报

2023年10月23日-2023年10月29日

2023年第43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 47 个，其中高危漏洞 187 个、中危漏洞 249 个、低危漏洞 11 个。漏洞平均分为 6.42。本周收录的漏洞中，涉及 0day 漏洞 387 个（占 87%），其中互联网上出现“Mediawiki 输入验证错误漏洞（CNVD-2023-79688）、Diafan 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漏洞总数 12213 个，与上周（11677 个）环比增多 5%。

### CNVD收录漏洞近10周平均分分布图

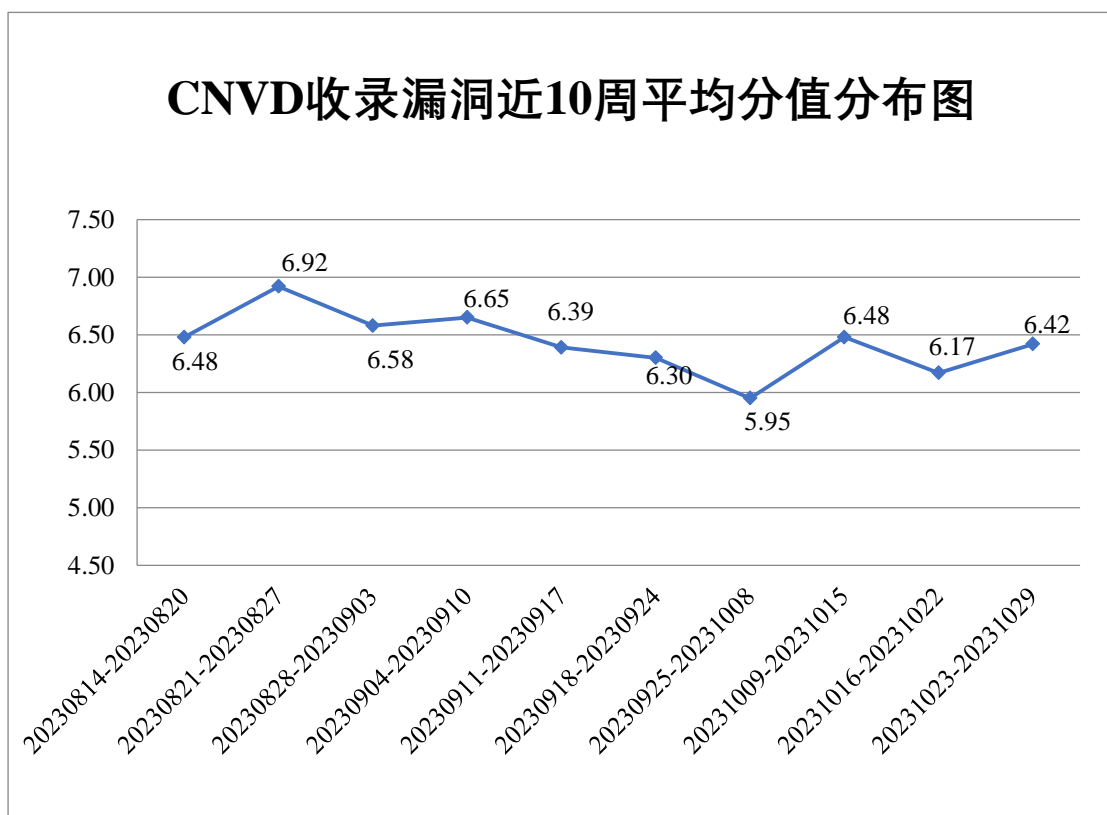



图 1 CNVD 收录漏洞近 10 周平均分分布图



## 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 27 起，向基础电信企业通报漏洞事件 12 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 1203 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 184 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 70 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：

淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、中磊电子（苏州）有限公司、郑州信泽华计算机技术开发有限公司、郑州天迈科技股份有限公司、正方软件股份有限公司、镇雄微生活网络科技文化传播有限公司、镇江市云优网络科技有限公司、浙江蓝巨星国际传媒有限公司、掌如科技服务有限公司、长沙巴巴开源网络科技有限公司、长春城投智慧城建科技有限公司、云内控科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、医惠科技有限公司、信诺瑞得（北京）科技有限公司、西门子（中国）有限公司、西安新软信息科技有限公司、武汉理工光科股份有限公司、武汉金同方科技有限公司、网是科技股份有限公司、网件（北京）网络技术有限公司、万洲电气股份有限公司、万熠科技有限公司、推想医疗科技股份有限公司、太原易思软件技术有限公司、索尼（中国）有限公司、随锐科技集团股份有限公司、四川众望升腾科技有限公司、四川省进取科技有限公司、烁东方传媒（北京）有限公司、世邦通信股份有限公司、深圳左邻永佳科技有限公司、深圳中台威堡科技有限公司、深圳心颜科技有限责任公司、深圳市优卡特实业有限公司、深圳市乙辰科技股份有限公司、深圳市网旭科技有限公司、深圳市麦斯杰网络有限公司、深圳市领空技术有限公司、深圳市科脉技术股份有限公司、深圳市捷视飞通科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市道尔智控科技股份有限公司、深圳市必联电子有限公司、深圳市邦建通讯设备有限公司、深圳警翼智能科技股份有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海云轴信息科技有限公司、上海跃橙文化传播有限公司、上海序言泽网络科技有限公司、上海熙软科技有限公司、上海微肯网络科技有限公司、上海牛之云科技有限公司、上海麦汇信息科技有限公司、上海建文软件有限公司、上海寰创通信科技股份有限公司、上海泛微网络科技股份有限公司、上海畅响自动化技术有限公司、上海布雷德科技有限公司、熵基科技股份有限公司、陕西小伙伴网络科技有限公司、山西联运集团股份有限公司、山东中创软件商用中间件股份有限公司、山东云时空信息科技有限公司、山东威尔数据股份有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、山东比特智能科技股份有限公司、厦门信用家网络科技有限公司、厦门四信通信科技有限公司、厦门狮子鱼网络科技有限公司、

三星(中国)投资有限公司、青岛叁度信息技术有限公司、青岛积成电子股份有限公司、青岛海信网络科技股份有限公司、普联技术有限公司、宁波万由电子科技有限公司、宁波江丰生物信息技术有限公司、南京帆软软件有限公司、南京博纳睿通软件科技有限公司、迈普通信技术股份有限公司、九州通医药集团股份有限公司、京晨科技股份有限公司、金富瑞(北京)科技有限公司、金蝶天燕云计算股份有限公司、金蝶软件(中国)有限公司、江苏金智教育信息股份有限公司、江苏安颐健康管理集团、佳能(中国)有限公司、吉翁电子(深圳)有限公司、吉林玉米中心批发市场有限公司、吉林省体思奇健康科技有限公司、慧星软件科技有限公司、惠普贸易(上海)有限公司、环球国际视频通讯社有限公司、华科网络技术开发、湖南建研信息技术股份有限公司、虹越花卉股份有限公司、河南日报报业集团有限公司、河南康派智能技术有限公司、河南诚实人实业集团有限责任公司、合肥达力信息科技有限公司、杭州易软共创网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州新视窗信息技术有限公司、杭州顺网科技股份有限公司、杭州三一谦成科技有限公司、杭州千宜科技有限公司、杭州海康威视数字技术股份有限公司、杭州冠航科技有限公司、杭州弗兰科信息安全科技有限公司、杭州安恒信息技术股份有限公司、海十联(杭州)智能科技有限公司、海南高济互联网医院有限公司、哈尔滨伟成科技有限公司、广州易凯软件技术有限公司、广州小橘灯信息科技有限公司、广州图创计算机软件开发有限公司、广州市雅天网络科技有限公司、广州市奥威亚电子科技有限公司、广州齐博网络科技有限公司、广西云鸟能源阶科技有限公司、广联达科技股份有限公司、广电运通金融电子股份有限公司、富士胶片商业创新(中国)有限公司、福州慧美丰科技有限公司、福建亿能达信息技术股份有限公司、福建顶点软件股份有限公司、凤凰汇信息科技有限公司、东蒙集团有限公司、东莞市益康企业策划有限公司、东莞市通天星软件科技有限公司、成都友加畅捷科技有限公司、成都阳洋福行实业有限公司、成都星锐蓝海网络科技有限公司、成都飞鱼星科技股份有限公司、常州新橙信息技术有限公司、彩讯科技股份有限公司、北京卓软在线信息技术有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京外研在线数字科技有限公司、北京通达信科科技有限公司、北京升鑫网络科技有限公司、北京睿智博创科技有限公司、北京人大金仓信息技术股份有限公司、北京球友圈网络科技有限公司、北京启明星辰信息安全技术有限公司、北京南北天地科技股份有限公司、北京络捷斯特科技发展股份有限公司、北京联达动力信息科技股份有限公司、北京雷石天地电子技术有限公司、北京京东叁佰陆拾度电子商务有限公司(京东)、北京金盘鹏图软件技术有限公司、北京金和网络股份有限公司、北京国双科技有限公司、北京道亨软件股份有限公司、北京辰信领创信息技术有限公司、北京车之家信息技术有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、安徽中技国医医疗科技有限公司、安徽旭帆信息科技有限公司、安徽回收郎物联科技有限公司、爱普生(中国)有限公司和 SEACMS。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、新华三技术有限公司、天津市国瑞数码安全系统股份有限公司、北京神州绿盟科技有限公司、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。杭州美创科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、联想集团、快页信息技术有限公司、安徽锋刃信息科技有限公司、亚信科技（成都）有限公司、河南东方云盾信息技术有限公司、湖南泛联新安信息科技有限公司、赛尔网络有限公司、江苏天竞云合数据技术有限公司、上海直画科技有限公司、内蒙古中叶信息技术有限责任公司、内蒙古洞明科技有限公司、北京微步在线科技有限公司、博智安全科技股份有限公司、北京天防安全科技有限公司、合肥梆梆信息科技有限公司、南京深安科技有限公司、北京六方云信息技术有限公司、北京君云天下科技有限公司、超聚变数字技术有限公司、成都愚安科技有限公司、信息产业信息安全测评中心、深圳昂楷科技有限公司、贵州多彩网安科技有限公司、中华人民共和国上海海事局、杭州默安科技有限公司、四川中成基业安全技术有限公司、安徽长泰科技有限公司、广州安亿信软件科技有限公司、江苏晟晖信息科技有限公司、上海观安信息技术股份有限公司、北京时代新威信息技术有限公司、西藏熙安信息技术有限责任公司、郑州埃文科技、江苏云天网络安全技术有限公司、北京华顺信安信息技术有限公司及其他个人白帽子向 CNVD 提交了 12213 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、三六零数字安全科技集团有限公司和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 10463 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
奇安信网神（补天平台）	6908	6908
斗象科技（漏洞盒子）	3001	3001
北京天融信网络安全技术有限公司	1413	23
新华三技术有限公司	619	0
天津市国瑞数码安全系统股份有限公司	509	0
北京神州绿盟科技有限公司	490	337
北京启明星辰信息安全	439	7

全技术有限公司		
上海交大	354	354
深信服科技股份有限公司	284	0
三六零数字安全科技集团有限公司	200	200
安天科技集团股份有限公司	180	0
阿里云计算有限公司	135	3
北京数字观星科技有限公司	132	0
中国电信股份有限公司网络安全产品运营中心	76	76
北京知道创宇信息技术有限公司	63	1
杭州安恒信息技术股份有限公司	48	1
京东科技信息技术有限公司	26	3
北京长亭科技有限公司	19	0
中电科网络安全科技股份有限公司	12	12
杭州迪普科技股份有限公司	10	0
南京联成科技发展股份有限公司	2	2
北京智游网安科技有限公司	2	2
恒安嘉新（北京）科技股份有限公司	1	0
北京升鑫网络科技有限公司（青藤云）	1	1
杭州美创科技有限公司	100	100

司		
奇安星城网络安全运营服务（长沙）有限公司	88	88
联想集团	70	70
快页信息技术有限公司	35	35
安徽锋刃信息科技有限公司	31	31
亚信科技（成都）有限公司	22	22
河南东方云盾信息技术有限公司	15	15
湖南泛联新安信息科技有限公司	6	6
赛尔网络有限公司	5	5
江苏天竞云合数据技术有限公司	4	4
上海直画科技有限公司	4	4
内蒙古中叶信息技术有限责任公司	3	3
内蒙古洞明科技有限公司	3	3
北京微步在线科技有限公司	3	3
博智安全科技股份有限公司	3	3
北京天防安全科技有限公司	2	2
合肥梆梆信息科技有限公司	2	2
南京深安科技有限公司	2	2
北京六方云信息技术	2	2

有限公司		
北京君云天下科技有限公司	2	2
超聚变数字技术有限公司	2	2
成都愚安科技有限公司	1	1
信息产业信息安全测评中心	1	1
深圳昂楷科技有限公司	1	1
贵州多彩网安科技有限公司	1	1
中华人民共和国上海海事局	1	1
杭州默安科技有限公司	1	1
四川中成基业安全技术有限公司	1	1
安徽长泰科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
江苏晟晖信息科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
北京时代新威信息技术有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
郑州埃文科技	1	1
江苏云天网络安全技术有限公司	1	1
北京华顺信安信息技	1	1

术有限公司		
CNCERT 广西分中心	19	19
CNCERT 河北分中心	4	4
CNCERT 贵州分中心	3	3
个人	836	836
报送总计	16206	12213

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 447 个漏洞。WEB 应用 228 个，应用程序 105 个，网络设备（交换机、路由器等网络端设备）76 个，智能设备（物联网终端设备）19 个，安全产品 15 个，操作系统 4 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	228
应用程序	105
网络设备（交换机、路由器等网络端设备）	76
智能设备（物联网终端设备）	19
安全产品	15
操作系统	4



## 本周CNVD漏洞数量按影响类型分布

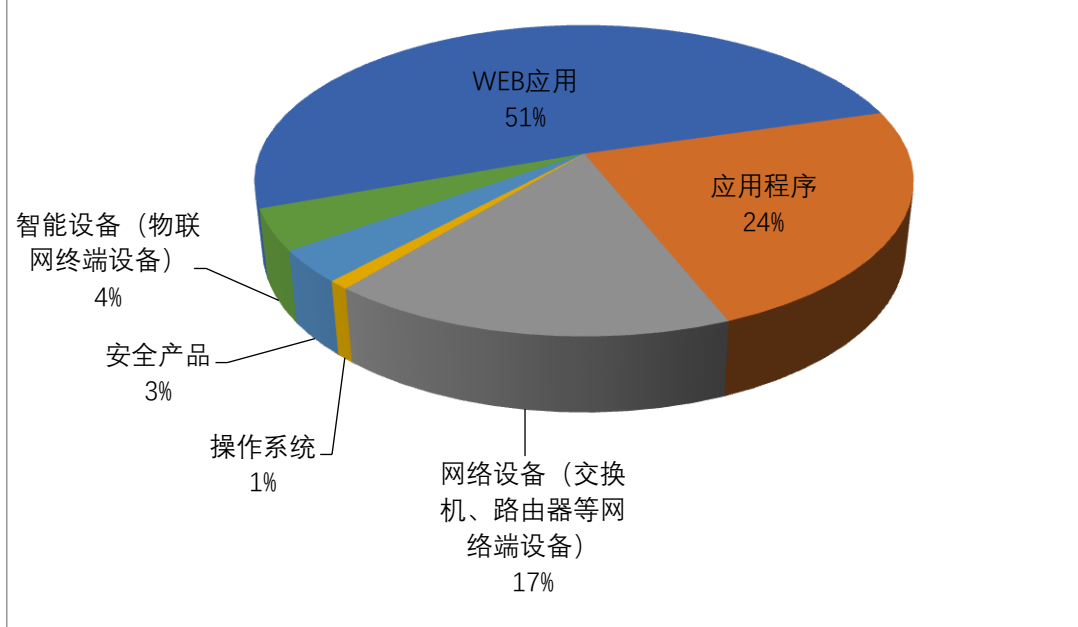


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及友讯电子设备（上海）有限公司、Apache、用友网络科技股份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	友讯电子设备（上海）有限公司	24	6%
2	Apache	14	3%
3	用友网络科技股份有限公司	11	2%
4	Microsoft	11	2%
5	IBM	9	2%
6	Cisco	8	2%
7	北京百卓网络技术有限公司	7	2%
8	WordPress	7	2%
9	上海卓卓网络科技有限公司	6	1%
10	其他	350	78%

本周，CNVD 收录了 26 个电信行业漏洞，41 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation Pavilion8 授权问题漏洞”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/>

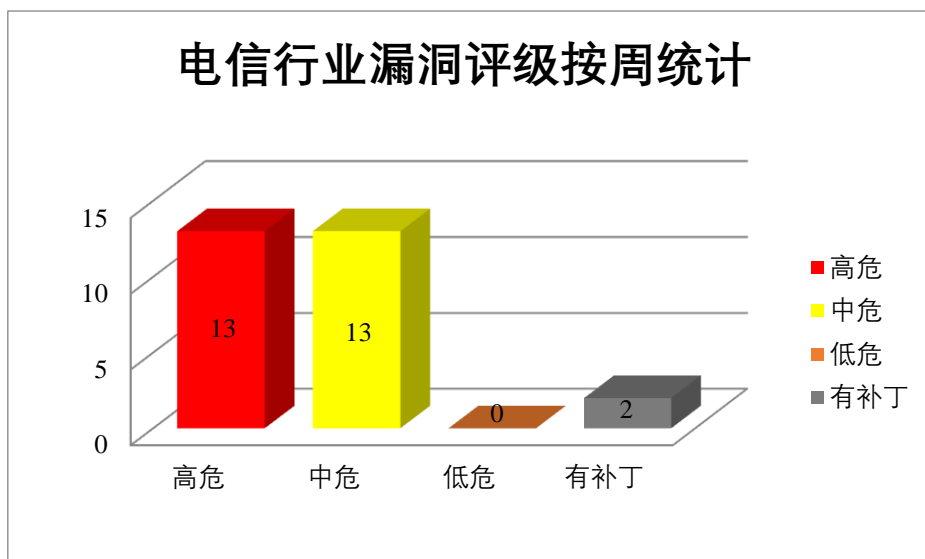


图 3 电信行业漏洞统计

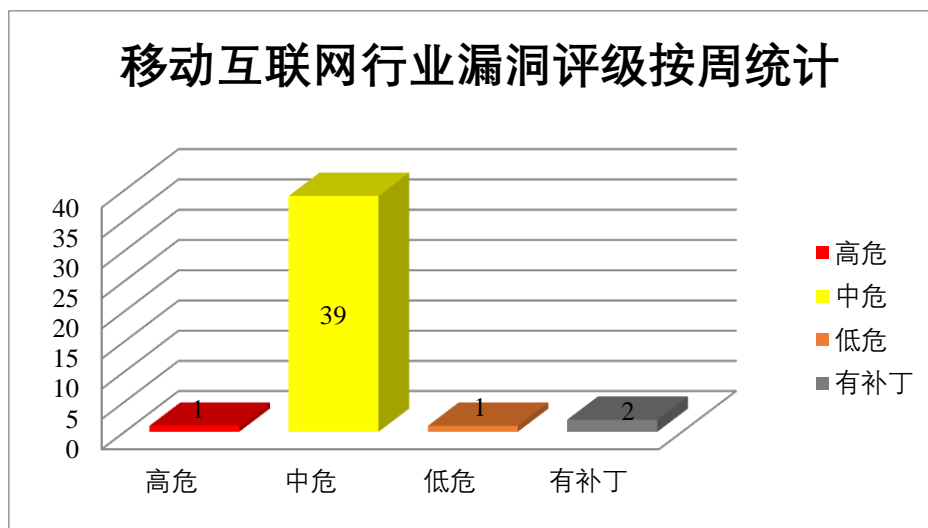


图 4 移动互联网行业漏洞统计

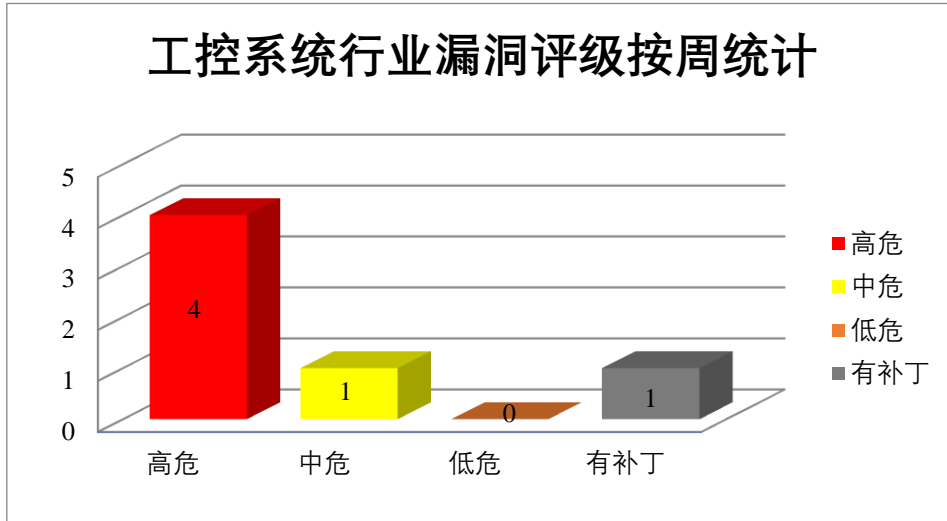


图 5 工控系统行业漏洞统计

## 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、IBM 产品安全漏洞

IBM App Connect Enterprise 是美国国际商业机器（IBM）公司的一个操作系统。IBM App Connect Enterprise 将现有业界信任的 IBM Integration Bus 技术与 IBM App Connect Professional 以及新的云本机技术进行了组合，提供一个可满足现代数字企业全面集成需求的平台。IBM Robotic Process Automation 是美国国际商业机器（IBM）公司的一种机器人流程自动化产品。IBM Integration Bus 是美国 IBM 公司的一款企业服务总线（ESB）产品。该产品为面向服务架构（SOA）环境和非 SOA 环境提供连通性和通用数据转换。IBM Sterling Partner Engagement Manager 是美国国际商业机器（IBM）公司的一个自动化工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从 API 日志中获取敏感信息，进行拒绝服务攻击，执行非法 SQL 命令获取数据库敏感数据。

CNVD 收录的相关漏洞包括：IBM App Connect Enterprise 信息泄露漏洞、IBM Robotic Process Automation 信息泄露漏洞（CNVD-2023-79713）、IBM App Connect Enterprise and IBM Integration Bus 拒绝服务漏洞、IBM Robotic Process Automation 授权问题漏洞（CNVD-2023-79715）、IBM Robotic Process Automation 安全绕过漏洞、IBM Robotic Process Automation 访问控制错误漏洞（CNVD-2023-79718）、IBM Sterling Partner Engagement Manager 拒绝服务漏洞、IBM Sterling Partner Engagement Manager SQL 注入漏洞。其中，“IBM Robotic Process Automation 访问控制错误漏洞（CNVD-2023-79718）”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-2023-79711>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79713>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79712>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79715>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79714>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79718>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79717>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79716>

## 2、Cisco 产品安全漏洞

Cisco DNA Center 是美国思科（Cisco）公司的一个网络管理和命令中心服务。Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实施相应策略来监管网络。Cisco Catalyst SD-WAN Manager 是一款开放、安全的云级架构管理控制台。Cisco vManage 是一个高度可定制的控制面板，可简化并自动执行 Cisco SD-WAN 部署、配置、管理与运营。Cisco Catalyst 是美国思科（Cisco）公司的一系列交换机。Cisco Emergency Responder 是美国思科（Cisco）公司的一款应急响应框架。Cisco Wireless LAN Controller（WLC）是美国思科（Cisco）公司的一款无线局域网控制器产品。该产品在无线局域网中提供安全策略、入侵检测等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，可读取和修改数据库数据，提升权限，读取、写入或删除底层操作系统上的任意文件，并将其权限升级为 root 等。

CNVD 收录的相关漏洞包括：Cisco DNA Center API 存在访问控制错误漏洞、Cisco Identity Services Engine 授权问题漏洞（CNVD-2023-79690）、Cisco Catalyst SD-WAN Manager 本地文件包含漏洞、Cisco Catalyst SD-WAN Manager 未授权访问漏洞、Cisco Catalyst SD-WAN Manager 授权绕过漏洞、Cisco Catalyst SD-WAN Manager HTML 注入漏洞、Cisco Emergency Responder 信任管理问题漏洞、Cisco Wireless LAN Controller 缓冲区溢出漏洞。其中，“Cisco DNA Center API 存在访问控制错误漏洞、Cisco Catalyst SD-WAN Manager 未授权访问漏洞、Cisco Catalyst SD-WAN Manager 授权绕过漏洞、Cisco Emergency Responder 信任管理问题漏洞”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-2023-79686>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79690>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80110>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80115>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80114>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80113>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80112>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80111>

### 3、Microsoft 产品安全漏洞

Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。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敏感信息，在系统上执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Excel 信息泄露漏洞（CNVD-2023-80108、CNVD-2023-80153）、Microsoft Excel 代码执行漏洞（CNVD-2023-80109、CNVD-2023-80162、CNVD-2023-80163、CNVD-2023-80164、CNVD-2023-80165）、Microsoft Excel 拒绝服务漏洞（CNVD-2023-80166）。其中，除“Microsoft Excel 信息泄露漏洞（CNVD-2023-80108、CNVD-2023-80153）、Microsoft Excel 拒绝服务漏洞（CNVD-2023-80166）”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-2023-80108>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80109>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80153>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80162>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80163>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80164>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80165>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80166>

### 4、Apache 产品安全漏洞

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 InLong 是美国阿帕奇（Apache）基金会的一站式海量数据集成框架。提供自动化、安全、可靠的数据传输能力。Apache Pulsar 是美国阿帕奇（Apache）基金会有一个用于云环境种，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 Jackrabbit 是美国阿帕奇（Apache）公司的一个内容存储库。Apache Helix 是美国阿帕奇（Apache）基金会有一个通用集群管理框架，用于自动管理托管在节点集群上的分区、复制和分布式资源。Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持。Apache Linkis 是美国阿帕奇（Apache）基金会有一个库。有助于轻松连接各种后端计算/存储引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行授权绕过，使

用代理的管理角色向任何话题生成消息，导致任意代码执行等。

CNVD 收录的相关漏洞包括：Apache Airflow 授权问题漏洞（CNVD-2023-80561）、Apache InLong 数据伪造问题漏洞、Apache InLong 代码问题漏洞、Apache Pulsar 授权问题漏洞、Apache Jackrabbit 代码执行漏洞、Apache Helix 反序列化漏洞、Apache Tomcat 开放重定向漏洞（CNVD-2023-80565）、Apache Linkis 代码执行漏洞（CNVD-2023-80566）。其中，除“Apache Airflow 授权问题漏洞（CNVD-2023-80561）、Apache InLong 数据伪造问题漏洞、Apache Tomcat 开放重定向漏洞（CNVD-2023-80565）”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-2023-80561>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80560>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80559>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80564>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80563>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80562>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80565>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-80566>

## 5、DedeBIZ 代码执行漏洞

DedeBIZ 是中国穆云智能科技（DedeBIZ）公司的一个内容管理系统。本周，DedeBIZ 被披露存在代码执行漏洞。攻击者可利用该漏洞导致任意代码执行。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-2023-80116>

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>

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-2023-79687	OpenCart 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://github.com/opencart/opencart/commit/0a8dd91e385f70e42795380009fd644224c1bc97">https://github.com/opencart/opencart/commit/0a8dd91e385f70e42795380009fd644224c1bc97</a>
CNVD-2023-80117	Dell Data Protection Central 加密问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202309-0000001638925158">https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202309-0000001638925158</a>
CNVD-2023	Mozilla Thunderbird 缓冲区	高	目前厂商已发布升级补丁以修复漏



-80118	溢出漏洞 (CNVD-2023-80118)		洞, 补丁获取链接: <a href="https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/">https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/</a>
CNVD-2023-80167	Microsoft Office 权限提升漏洞 (CNVD-2023-80167)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36569">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36569</a>
CNVD-2023-80558	Apache HTTP Server 缓冲区溢出漏洞 (CNVD-2023-80558)	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: <a href="http://d.apache.org/security/vulnerabilities_24.html">http://d.apache.org/security/vulnerabilities_24.html</a>
CNVD-2023-79689	Rockwell Automation Pavilion8 授权问题漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140590">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140590</a>
CNVD-2023-79718	IBM Robotic Process Automation 访问控制错误漏洞 (CNVD-2023-79718)	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: <a href="https://www.ibm.com/support/pages/node/6852663">https://www.ibm.com/support/pages/node/6852663</a>
CNVD-2023-80109	Microsoft Excel 代码执行漏洞 (CNVD-2023-80109)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33161">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33161</a>
CNVD-2023-80566	Apache Linkis 代码执行漏洞 (CNVD-2023-80566)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://lists.apache.org/thread/o682wz1ggq491ybvjwokxvcdtnzo76ls/">https://lists.apache.org/thread/o682wz1ggq491ybvjwokxvcdtnzo76ls/</a>
CNVD-2023-80564	Apache Pulsar 授权问题漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://lists.apache.org/thread/v39hqtgrmyxr85rmofwvgrktnflbq3q5">https://lists.apache.org/thread/v39hqtgrmyxr85rmofwvgrktnflbq3q5</a>

小结: 本周, IBM 产品被披露存在多个漏洞, 攻击者可利用漏洞从 API 日志中获取敏感信息, 进行拒绝服务攻击, 执行非法 SQL 命令获取数据库敏感数据。此外, Cisco、Microsoft、Apache 等多款产品被披露存在多个漏洞, 攻击者可利用漏洞提交特殊的请求, 可读取和修改数据库数据, 提升权限, 读取、写入或删除底层操作系统上的任意文件, 并将其权限升级为 root 等。另外, DedeBIZ 被披露存在代码执行漏洞。攻击者可利用该漏洞导致任意代码执行。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、Mediawiki 输入验证错误漏洞（CNVD-2023-79688）

### 验证描述

MediaWiki 是美国维基媒体（MediaWiki）基金会的一套自由免费的基于网络的 Wiki 引擎。该产品可用于部署内部的知识管理和内容管理系统。

Mediawiki v1.40.0 版本存在输入验证错误漏洞，该漏洞源于不验证 XML 文件中使用的命名空间。攻击者可利用该漏洞通过向实例管理员发送恶意链接来成为管理员。

### 验证信息

POC 链接：<https://fluidattacks.com/advisories/blondie/>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2023-79688>

### 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. Cloudflare 发现超容量 HTTP DDoS 攻击激增

Cloudflare 表示，2023 年第三季度记录的超容量 HTTP DDoS（分布式拒绝服务）攻击数量超过了往年，这表明威胁格局已进入新的篇章。

参考链接：<https://www.bleepingcomputer.com/news/security/cloudflare-sees-surge-in-higher-volumetric-http-ddos-attacks/>

### 2. Chrome 更新传播特洛伊木马恶意软件

欺诈性 Chrome 更新网站的惊人激增引起了人们的关注，因为它们可能通过远程访问木马未经授权访问用户的设备。

参考链接：<https://cybernews.com/news/chrome-update-trojan-malware/>

## 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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82991537