国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 09 月 04 日-2023 年 09 月 10 日 **2023 年第 36 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 366 个，其中高危漏洞 159 个、中危漏洞 200 个、低危漏洞 7 个。漏洞平均分值为 6.65。本周收录的漏洞中，涉及 0day 漏洞 274 个（占 75%），其中互联网上出现“Online Travel Agency System 跨站脚本漏洞、XXL-JOB 跨站请求伪造漏洞（CNVD-2023-67068）”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 16173 个，与上周（13976 个）环比增多 16%。

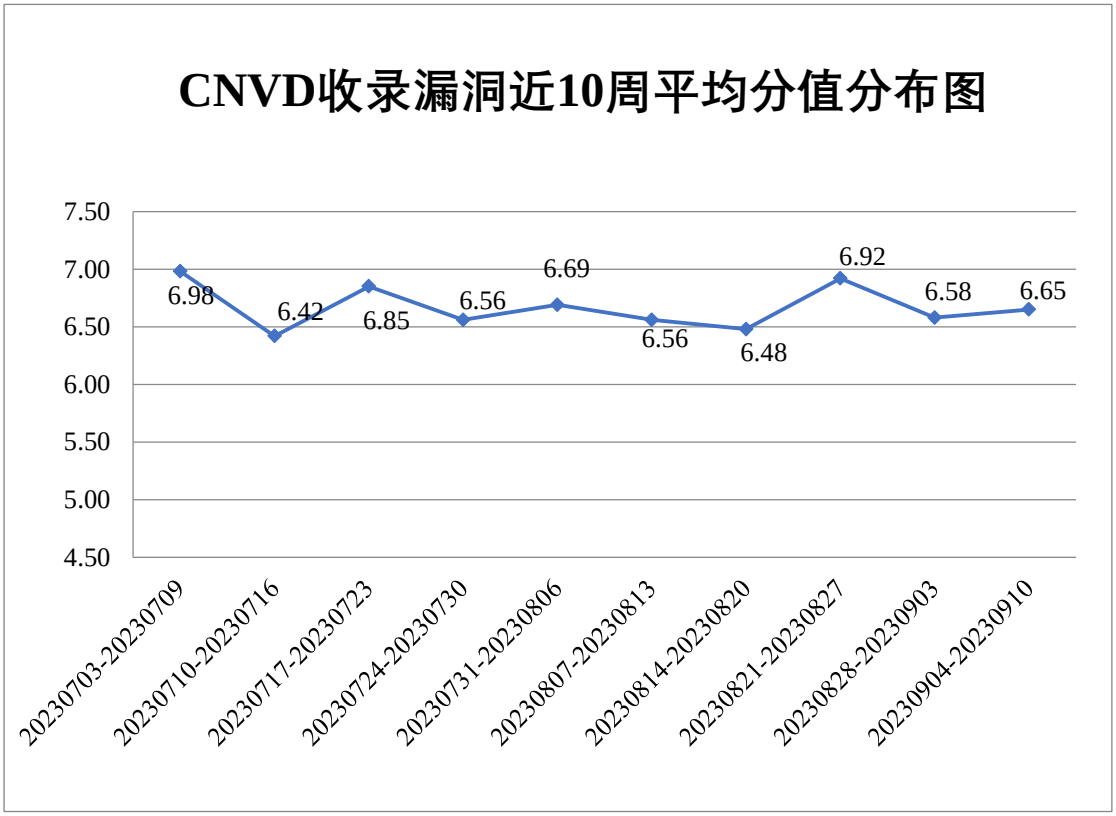

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 30 起，向基础电信企业通报漏洞事件 14 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 1056 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 157 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 59 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：

珠海市世源光电科技有限公司、珠海金山办公软件有限公司、珠海奔图电子有限公司、重庆远秋科技股份有限公司、众勤通信设备贸易（上海）有限公司、中控泰科（北京）科技发展有限公司、中科方德软件有限公司、中国卫通集团股份有限公司、中孚信息股份有限公司、浙江美术传媒拍卖有限公司、浙江大华技术股份有限公司、云南入目三分科技有限公司、远孚物流集团有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易事特集团股份有限公司、央广小品科技（北京）有限公司、新开普电子股份有限公司、小明太极（湖北）国漫文化有限公司、西安三才科技实业有限公司、西安交大捷普网络科技有限公司、西安大西信息科技有限公司、武汉益模科技股份有限公司、武汉天喻软件有限公司、武汉天地伟业科技有限公司、武汉达梦数据库有限公司、无锡信捷电气股份有限公司、天闻数媒科技（北京）有限公司、天维尔信息科技股份有限公司、天津市金匮灵兰科技有限公司、天津生态城投资开发有限公司、天津南大通用数据技术股份有限公司、腾讯安全应急响应中心、太原易思软件技术有限公司、索尼（中国）有限公司、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、四创科技有限公司、世茂天成物业服务集团有限公司、神彩科技股份有限公司、深圳坐标软件集团有限公司、深圳智慧光迅信息技术有限公司、深圳致软信息技术有限公司、深圳市亿图软件有限公司、深圳市乙辰科技股份有限公司、深圳市雄帝科技股份有限公司、深圳市明源云科技有限公司、深圳市明源软件股份有限公司、深圳市领空技术有限公司、深圳市朗驰欣创科技股份有限公司、深圳市科脉技术股份有限公司、深圳市科陆电子科技股份有限公司、深圳市佳峰珠宝首饰有限公司、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、深圳神一健康管理有限公司、深圳华视美达信息技术有限公司、深圳典阅科技有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海焱灿网络科技有限公司、上海善居电子商务有限公司、上海人宝实业集团有限公司、上海派琪网络科技有限公司、上海穆云智能科技有限公司、上海灵当信息科技有限公司、上海皇家网络科技有限公司、上海亘岩网络科技有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海必智科技有限公司、熵基科技股份有限公司、陕西锦华网络科技有限责任公司、山脉科技股份有限公司、山东潍大软件有

限公司、山东手麦智能科技有限公司、山东仁科测控技术有限公司、山东科德电子有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、厦门人众软件科技有限公司、赛维斯智慧环境科技（山东）有限公司、青岛海信网络科技股份有限公司、普元信息技术股份有限公司、普联技术有限公司、鹏为软件股份有限公司、牛迈网络科技有限公司、内蒙古锦贤物流有限公司、南通云尚找家纺电子商务有限公司、南京云网汇联软件技术有限公司、南京壹证通信息科技有限公司、迈普通信技术股份有限公司、流光星际（湖北）科技有限公司、廊坊和易生活网络科技股份有限公司、竣禾科技有限公司、精华教育科技股份有限公司、江西铭软科技有限公司、江西居购网络科技有限公司、江苏中天互联科技有限公司、吉林修正堂药房连锁经营有限公司、淮南市银泰软件科技有限公司、淮南市讯网信息技术有限公司、湖南千山慢病健康管理有限公司、湖南康通电子股份有限公司、湖南佰吉泰网络科技有限公司、合肥盛东信息科技有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、杭州观远数据有限公司、哈尔滨伟成科技有限公司、广州同望科技发展有限公司、广州市保伦电子有限公司、广州联享信息科技有限公司、广联达科技股份有限公司、广东百沃信息技术服务有限公司、富士胶片商业创新（中国）有限公司、福建奇鹭物联网科技股份公司、成都武侯环亚华康体检门诊部有限公司、成都萌想科技有限责任公司、成都风腾伟业科技有限公司、常熟纺支宝科技有限公司、禅道软件（青岛）有限公司、北京智慧远景科技产业有限公司、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、北京信安世纪科技有限公司、北京网御星云信息技术有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京趣拿信息技术有限公司、北京朗新天霁软件技术有限公司、北京九思协同软件有限公司、北京金盘鹏图软件技术有限公司、北京宏景世纪软件股份有限公司、北京国文信文物保护有限公司、北京国通创投信息科技有限公司、北京国炬信息技术有限公司、北京高速波软件有限公司、北京辰安科技股份有限公司、北京碧海威科技有限公司、北京北大方正电子有限公司、北京佰才邦技术股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、百旺金穗云信息科技有限公司、傲拓科技股份有限公司、安徽生命港湾信息技术有限公司、阿里巴巴集团安全应急响应中心、zzzcms 和 SEMCMS。

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、北京天融信网络安全技术有限公司、新华三技术有限公司、安天科技集团股份有限公司、中国电信股份有限公司网络安全产品运营中心等单位报送公开收集的漏洞数量较多。上海齐同信息科技有限公司、联想集团、博智安全科技股份有限公司、河南东方云盾信息技术有限公司、安徽锋刃信息科技有限公司、海南大学、奇安星城网络安全运营服务（长沙）

有限公司、河南灵创电子科技有限公司、中电智安科技有限公司、快页信息技术有限公司、亚信科技（成都）有限公司、赛尔网络有限公司、中国电信股份有限公司上海研究院、信息产业信息安全测评中心、河南悦海数安科技有限公司、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、北京微步在线科技有限公司、国网江西省电力有限公司电力科学研究院、北京时代新威信息技术有限公司、山东云天安全技术有限公司、建信金科网络攻击实验室、江苏极元信息技术有限公司、苏州棱镜七彩信息科技有限公司、北京云弈科技有限公司、中孚安全技术有限公司、北京山石网科信息技术有限公司、长春嘉诚信息技术股份有限公司、宁夏凯信特信息科技有限公司、软通动力信息技术（集团）股份有限公司、北京威努特技术有限公司、南京赛宁信息技术有限公司、墨菲未来科技（北京）有限公司及其他个人白帽子向 CNVD 提交了 16173 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、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 14545 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）	11135	11135
奇安信网神（补天平台）	1907	1907
上海交大	758	758
三六零数字安全科技集团有限公司	745	745
北京启明星辰信息安全技术有限公司	620	0
北京天融信网络安全技术有限公司	501	0
新华三技术有限公司	439	0
安天科技集团股份有限公司	300	1
中国电信股份有限公司网络安全产品运营中心	176	176
北京知道创宇信息技术有限公司	119	0
北京数字观星科技有限公司	117	0
深信服科技股份有限	114	0

公司		
阿里云计算有限公司	106	2
杭州安恒信息技术股份有限公司	89	0
北京长亭科技有限公司	80	0
远江盛邦（北京）网络安全科技股份有限公司	22	22
杭州迪普科技股份有限公司	22	0
京东科技信息技术有限公司	5	5
华为技术有限公司	2	2
北京神州绿盟科技有限公司	1	1
上海齐同信息科技有限公司	177	177
联想集团	84	84
博智安全科技股份有限公司	47	47
河南东方云盾信息技术有限公司	40	40
安徽锋刃信息科技有限公司	28	28
海南大学	25	25
奇安星城网络安全运营服务（长沙）有限公司	23	23
河南灵创电子科技有限公司	19	19
中电智安科技有限公司	18	18
快页信息技术有限公司	16	16

亚信科技（成都）有限公司	12	12
赛尔网络有限公司	5	5
中国电信股份有限公司上海研究院	5	5
信息产业信息安全测评中心	3	3
河南悦海数安科技有限公司	3	3
广州安亿信软件科技有限公司	3	3
江苏晟晖信息科技有限公司	3	3
北京微步在线科技有限公司	2	2
国网江西省电力有限公司电力科学研究院	2	2
北京时代新威信息技术有限公司	2	2
山东云天安全技术有限公司	2	2
建信金科网络攻击实验室	2	2
江苏极元信息技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
北京云弈科技有限公司	1	1
中孚安全技术有限公司	1	1
北京山石网科信息技术有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1

宁夏凯信特信息科技有限公司	1	1
软通动力信息技术（集团）股份有限公司	1	1
北京威努特技术有限公司	1	1
南京赛宁信息技术有限公司	1	1
墨菲未来科技（北京）有限公司	1	1
CNCERT 宁夏分中心	3	3
个人	884	884
报送总计	18677	16173

本周漏洞按类型和厂商统计

本周，CNVD 收录了 366 个漏洞。WEB 应用 186 个，应用程序 87 个，网络设备（交换机、路由器等网络端设备）53 个，数据库 20 个，操作系统 9 个，智能设备（物联网终端设备）6 个，安全产品 5 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	186
应用程序	87
网络设备（交换机、路由器等网络端设备）	53
数据库	20
操作系统	9
智能设备（物联网终端设备）	6
安全产品	5

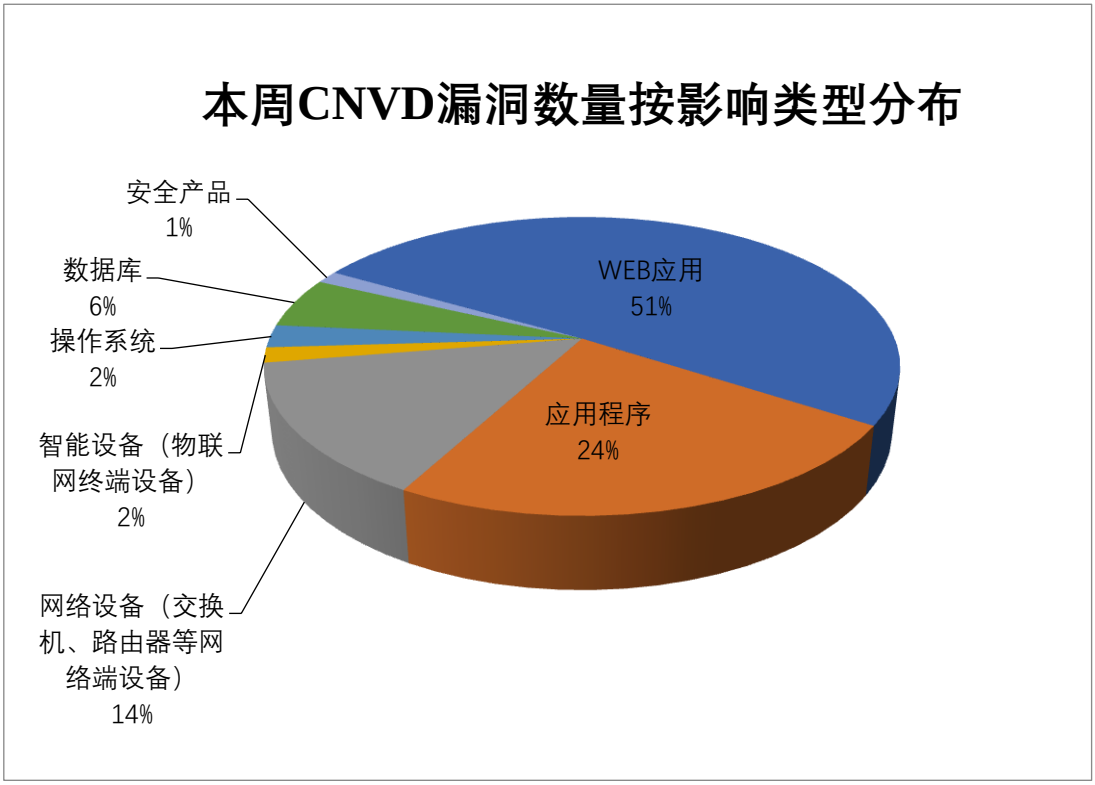

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京通达信科科技有限公司、Oracle、Apache 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	北京通达信科科技有限公司	23	6%
2	Oracle	20	5%
3	Apache	12	3%
4	D-Link	12	3%
5	IBM	11	3%
6	Mozilla	11	3%
7	FreeImage	10	3%
8	Google	10	3%
9	成都德芯数字科技股份有限公司	6	2%
10	其他	251	69%

本周行业漏洞收录情况

本周，CNVD 收录了 47 个电信行业漏洞，28 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，“Oracle MySQL Server 拒绝服务漏洞（CNVD-2023-6

7110）”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/

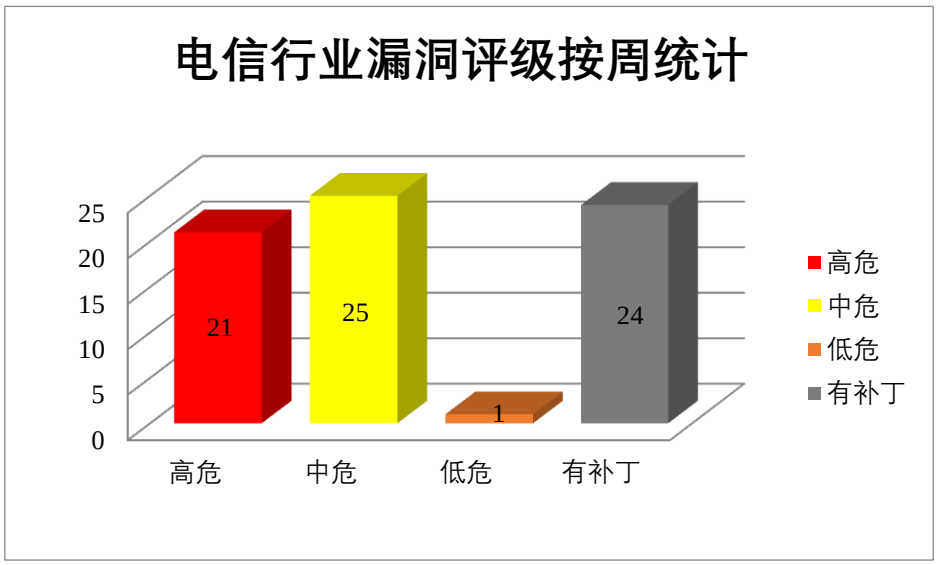

图 3 电信行业漏洞统计

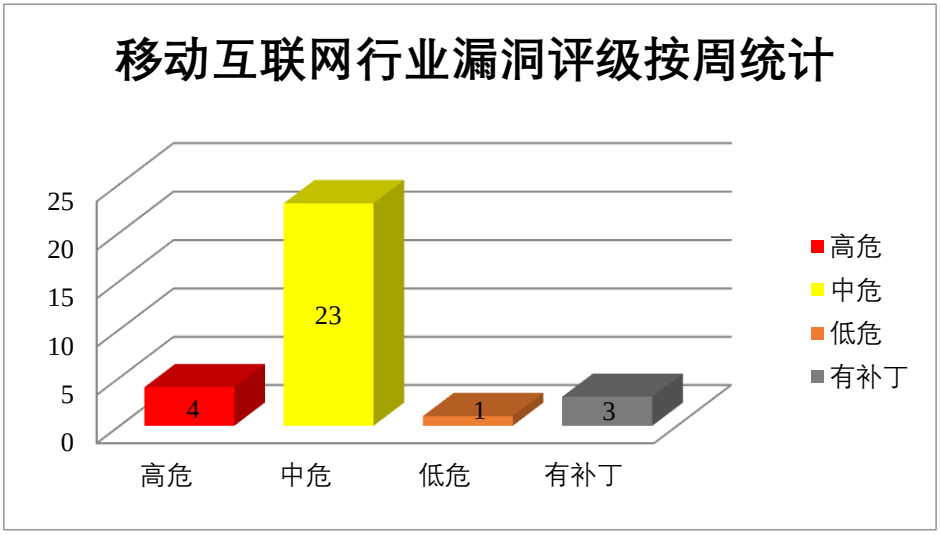

图 4 移动互联网行业漏洞统计

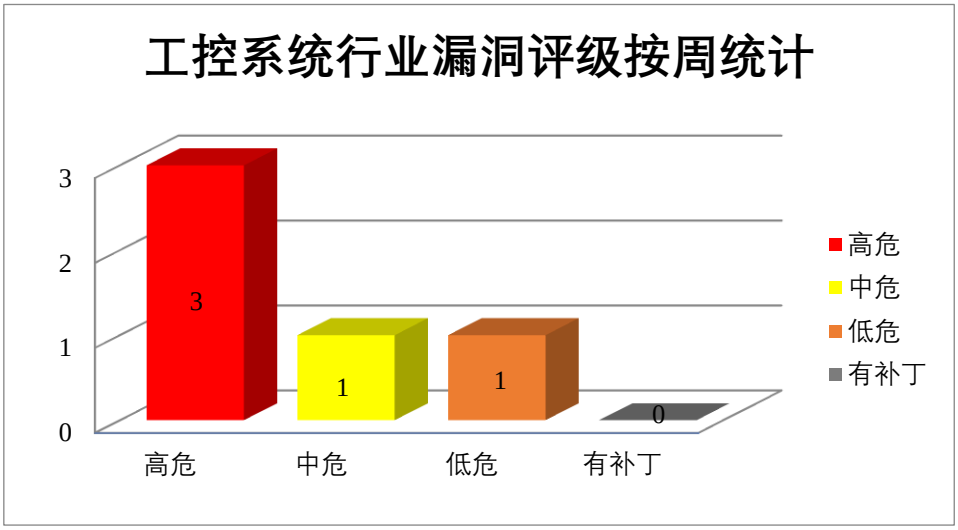

图 5 工控系统行业漏洞统计

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 Security Guardium 是美国国际商业机器（IBM）公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过发送特制的 HTTP 请求来枚举用户名，发送特制请求在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：IBM Security Guardium 信息泄露漏洞（CNVD-2023-66732）、IBM Security Guardium SQL 注入漏洞（CNVD-2023-66731）、IBM Security Guardium 跨站脚本漏洞（CNVD-2023-66735、CNVD-2023-66734、CNVD-2023-66733）、IBM Security Guardium 命令执行漏洞（CNVD-2023-66738、CNVD-2023-66736）、IBM Security Guardium 身份验证错误漏洞。其中，“IBM Security Guardium 命令执行漏洞（CNVD-2023-66738、CNVD-2023-66736）、IBM Security Guardium 身份验证错误漏洞”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-2023-66732

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66731

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66735

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66734

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66733

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66738

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66737

https://www.cnvd.org.cn/flaw/show/CNVD-2023-66736

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，在系统上执行任意代码或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2023-67083）、Google Chrome FedCM 安全绕过漏洞、Google Chrome navigation 安全绕过漏洞（CNVD-2023-67085）、Google Chrome WebShare 安全绕过漏洞、Google Chrome Accessibility 信息泄露漏洞、Google Chrome Browser History 缓冲区溢出漏洞、Google Chrome Vulkan 代码执行漏洞、Google Chrome Intents 安全绕过漏洞。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-2023-67083

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67084

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67085

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67086

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67087

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67088

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67089

https://www.cnvd.org.cn/flaw/show/CNVD-2023-67090

3、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 ShardingSphere 是美国阿帕奇（Apache）基金会的一套开源的分布式数据库中间件解决方案。Apache Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。Apache EventMesh 是美国阿帕奇（Apache）基金会的新一代无服务器事件中间件，用于构建分布式事件驱动应用程序。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 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 Accumulo 是美国阿帕奇（Apache）基金会的一个可靠的、可伸缩的、高性能的排序分布式的 Key-Value 存储应用。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，通过无效的 Range 标头导致崩溃，通过构建特殊的 YAML 配置文件来执行任意代码等。

CNVD 收录的相关漏洞包括：Apache Airflow 输入验证错误漏洞（CNVD-2023-67067）、Apache ShardingSphere 反序列化漏洞、Apache Airflow 授权问题漏洞（CNVD-2023-67070）、Apache Traffic Server 输入验证错误漏洞（CNVD-2023-67069）、Apache EventMesh 反序列化漏洞、Apache Pulsar 信息泄露漏洞、Apache Tomcat 信息泄露漏洞（CNVD-2023-67080）、Apache Accumulo 授权问题漏洞。其中，除“Apache Pulsar 信息泄露漏洞”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-2023-67067
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67071
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67070
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67069
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67072
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67076
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67080
https://www.cnvd.org.cn/flaw/show/CNVD-2023-67079

4、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Firefox ESR 是火狐浏览器(企业版)。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从此文件夹中读取文件并获得对潜在敏感信息的访问权限，导致程序崩溃，任意代码执行等。

CNVD 收录的相关漏洞包括：Mozilla Firefox and Firefox ESR 缓冲区溢出漏洞、Mozilla Firefox 内存错误引用漏洞（CNVD-2023-68209） 、Mozilla Firefox 访问控制错误漏洞（CNVD-2023-68217）、Mozilla Firefox 输入验证错误漏洞（CNVD-2023-68216）、Mozilla Firefox 内存破坏漏洞（CNVD-2023-68215）、Mozilla Thunderbird 和 Firefox 任意代码执行漏洞、Mozilla Thunderbird 资源管理错误漏洞（CNVD-2023-68219）、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-68218）。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-2023-68210
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68209
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68217
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68216
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68215
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68214

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68219

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68218

5、tenda AC6 缓冲区溢出漏洞（CNVD-2023-68221）

Tenda AC6 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC6 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务攻击。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-2023-68221

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-2023-67081	HTMLDOC 缓冲区溢出漏洞（CNVD-2023-67081）	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/michaelrsweet/htmldoc/commit/c67bbd8756f015e33e4ba639a40c7f9d8bd9e8ab
CNVD-2023-67113	FreeImage C_IStream::read 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/300/
CNVD-2023-67114	FreeImage FreeImage_CloneTag 函数拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/335/
CNVD-2023-68416	Apple 多款产品存在任意代码执行漏洞（CNVD-2023-68416）	高	厂商已发布了更新版本修复漏洞，建议受影响用户升级至将相关 Apple 产品升级至 iOS 16.6.1、iPadOS 16.6.1、macOS Ventura 13.5.2 和 watchOS 9.6.2。新版本可在系统更新推送中找到，请及时关注更新：https://www.apple.com.cn/
CNVD-2023-67116	FreeImage LoadRGB 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/299/
CNVD-2023-67117	FreeImage LoadPixelDataRLE8 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/298/
CNVD-2023	Apple 多款产品任意代码执行	高	厂商已发布了更新版本修复漏洞，

-68417	漏洞		建议受影响用户升级至将相关 Apple 产品升级至 iOS 16.6.1、iPadOS 16.6.1、macOS Ventura 13.5.2。新版本可在系统更新推送中找到，请及时关注更新：https://www.apple.com.cn/
CNVD-2023-67119	FreeImage ofLoad 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/337/
CNVD-2023-68223	Exiv2 缓冲区溢出漏洞（CNVD-2023-68223）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Exiv2/exiv2/releases/tag/v0.28.0
CNVD-2023-68224	ImageMagick 拒绝服务漏洞（CNVD-2023-68224）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ImageMagick/ImageMagick/pull/4098

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞通过发送特制的 HTTP 请求来枚举用户名，发送特制请求在系统上执行任意命令等。此外，Google、Apache、Mozilla 等多款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，通过无效的 Range 标头导致崩溃，通过构建特殊的 YAML 配置文件来执行任意代码等。另外，Tenda AC6 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或者导致拒绝服务攻击。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、Online Travel Agency System 跨站脚本漏洞

验证描述

Online Travel Agency System 是一个在线旅行社系统。

Online Travel Agency System v1.0 版本存在跨站脚本漏洞，该漏洞源于 insert.php 的参数 description 对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞可以通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/DiliLearngent/BugReport/blob/main/php/Online-Travel-Agency-System/bug9-XSS-description.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-67066

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. Google 开始对更多 Chrome 用户启用隐私沙盒

隐私沙盒（Privacy Sandbox）将取代第三方 Cookie，它通过用户的浏览历史跟踪用户的兴趣，允许广告商根据兴趣展示广告，而用户可以管理兴趣并对其归类分组。

参考链接：https://arstechnica.com/gadgets/2023/09/googles-widely-opposed-ad-platform-the-privacy-sandbox-launches-in-chrome/

2. 苹果修复了一个正被利用的零点击 0day 漏洞

加拿大多伦多大学公民实验室的研究人员在检查一部 iPhone 手机时，发现了一个零点击 0day 漏洞正被利用感染以色列公司 NSO Group 的间谍软件 Pegasus。苹果已经释出了 iOS 16.6.1 修复漏洞。研究人员表示会在未来公布漏洞利用的更多细节。

参考链接：https://www.solidot.org/story?sid=76023

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