

## 信息安全漏洞周报

2023年07月03日-2023年07月09日

2023年第27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 475 个，其中高危漏洞 306 个、中危漏洞 157 个、低危漏洞 12 个。漏洞平均分为 6.98。本周收录的漏洞中，涉及 0day 漏洞 410 个（占 86%），其中互联网上出现“novel-plus 文件上传漏洞、Personnel Property Equipment System 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 7156 个，与上周（7988 个）环比减少 10%。

### CNVD收录漏洞近10周平均分分布图

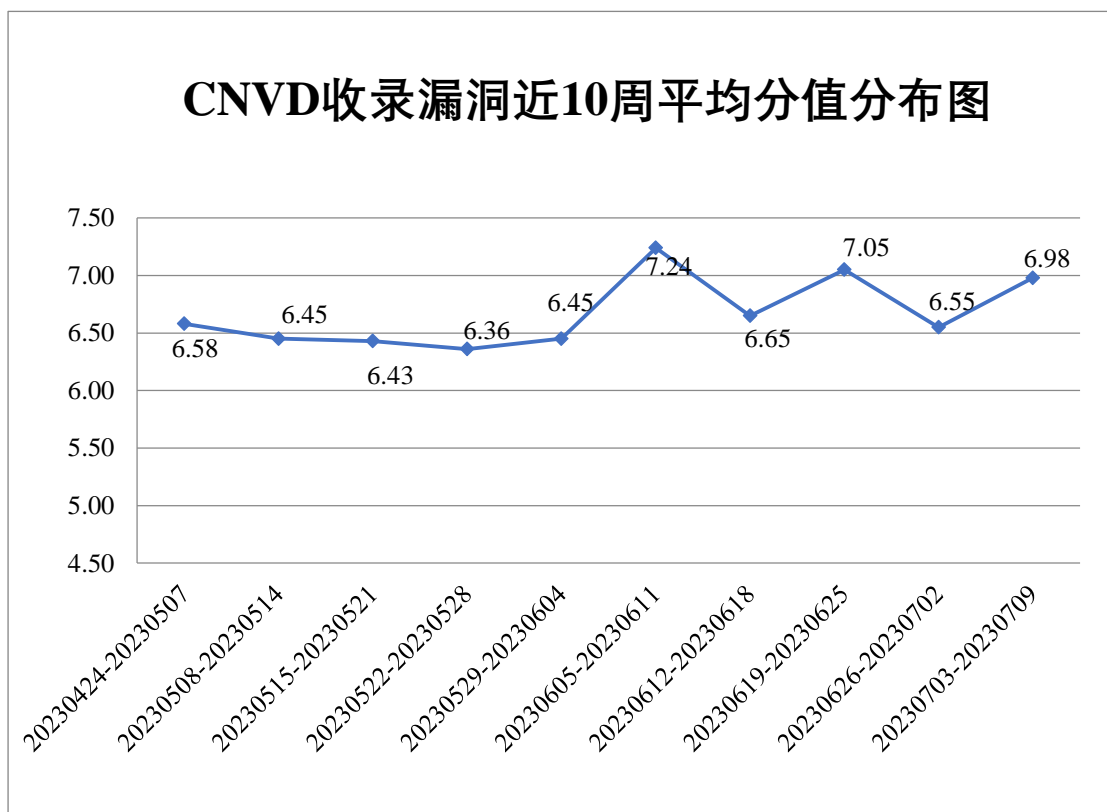



图 1 CNVD 收录漏洞近 10 周平均分分布图



## 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 28 起，向基础电信企业通报漏洞事件 16 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 647 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 117 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 58 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：

重庆与异或科技有限公司、中金亚洲（北京）国际互联网科技有限公司、智互联（深圳）科技有限公司、浙江新再灵科技股份有限公司、掌如科技服务有限公司、长沙巴巴开源网络科技有限公司、元生软件科技（广东）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、新开普电子股份有限公司、新华三智能终端有限公司、武汉金同方科技有限公司、潍坊滨海人才发展集团有限公司、崑远科技股份有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、梯子数字文化扬州有限公司、腾讯安全应急响应中心、台达集团、苏州盛科通信股份有限公司、苏州宏云智能科技有限公司、四川三德信息技术有限责任公司、神州数码控股有限公司、深圳市兴海物联科技有限公司、深圳市思迅软件股份有限公司、深圳市双梦科技有限公司、深圳市尼高企业形象设计有限公司、深圳市漫步者科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市海融易通电子有限公司、深圳市鼎微科技有限公司、深圳市顶讯网络科技有限公司、深圳市艾森互动科技有限公司、深圳华视美达信息技术有限公司、深圳邦健生物医疗设备股份有限公司、上海卓卓网络科技有限公司、上海卓越睿新数码科技股份有限公司、上海洲马网络科技有限公司、上海英立视数字科技有限公司、上海喜马拉雅科技有限公司、上海力软信息技术有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海酆泽信息技术有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、上海百胜软件股份有限公司、上海艾泰科技有限公司、上海阿法迪智能数字科技股份有限公司、熵基科技股份有限公司、山脉科技股份有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、山东广安车联科技股份有限公司、山东德尔智能数码股份有限公司、山东博硕自动化技术有限公司、厦门姿致健康科技有限公司、若依、青岛中瑞云数科技有限公司、青岛易软天创网络科技有限公司、普联技术有限公司、平行云科技（北京）有限公司、诺亚机器人科技（上海）有限公司、宁波畅想软件股份有限公司、南京霍普斯科技有限公司、迈普通信技术股份有限公司、浪潮电子信息产业股份有限公司、蓝网科技股份有限公司、酷溜网（北京）科技有限公司、金华聚秀科技有限公司、金蝶软件（中国）有限公司、江苏省农垦农业发展股份有限公司、湖南畅远信息技术有限公司、河南中视云

计算有限公司、河南易税科技有限公司、河北华安科技开发有限公司、合肥千界文化传媒有限公司、合肥贰道网络科技有限公司、杭州叙简科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州美创科技股份有限公司、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、杭州迪普科技股份有限公司、杭州安恒信息技术股份有限公司、海南赞赞网络科技有限公司、广州图创计算机软件开发有限公司、广联达科技股份有限公司、富盛科技股份有限公司、成都同飞科技有限责任公司、成都天问互联科技有限公司、成都青软青之软件有限公司、成都每经传媒有限公司、畅捷通信息技术股份有限公司、毕孚自动化设备贸易(上海)有限公司、北京字节跳动科技有限公司、北京致远互联软件股份有限公司、北京志凌海纳科技有限公司、北京一亩田新农网络科技有限公司、北京二零二四精英教育科技有限公司、北京西控电子商务有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京快学在线教育科技有限公司、北京凯特伟业科技有限公司、北京九思协同软件有限公司、北京竞业达数码科技股份有限公司、北京金和网络股份有限公司、北京杰控科技有限公司、北京豆牛网络科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、奥琦玮信息科技(北京)有限公司、安美世纪(北京)科技有限公司、安科瑞电气股份有限公司、安徽旭帆信息科技有限公司、阿里巴巴集团安全应急响应中心、山东文旅云智能科技有限公司、voidtools、semcms 和 ABLELink。

## 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、安天科技集团股份有限公司、深信服科技股份有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。内蒙古中叶信息技术有限责任公司、杭州美创科技有限公司、河南东方云盾信息技术有限公司、河南信安世纪科技有限公司、快页信息技术有限公司、奇安星城网络安全运营服务(长沙)有限公司、联想集团、安徽锋刃信息科技有限公司、杭州默安科技有限公司、重庆电信系统集成有限公司、内蒙古洞明科技有限公司、赛尔网络有限公司、广州安亿信软件科技有限公司、河南省鼎信信息安全等级测评有限公司、河北镌远网络科技有限公司、浙江木链物联网科技有限公司、江苏极元信息技术有限公司、宁夏凯信特信息科技有限公司、中能融合智慧科技有限公司、北京网御星云信息技术有限公司、西藏熙安信息技术有限责任公司、奇安信-工控安全实验室、德国电信咨询公司中国区公司、四川中成基业安全技术有限公司、南京师范大学常州创新发展研究院软件与信息安全测评中心、博智安全科技股份有限公司、郑州埃文科技、工业和信息化部电子第五研究所、北京山石网科信息技术有限公司、安徽长泰科技有限公司、重庆易阅科技有限公司、亚信科技(成都)有限公司及其他个人白帽子向 CNVD 提交了 7156 个以事件型漏洞为主的原创漏洞，其中包括奇

安信网神（补天平台）、斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 5192 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）	3452	3452
奇安信网神（补天平台）	1127	1127
上海交大	613	613
北京启明星辰信息安全技术有限公司	565	2
安天科技集团股份有限公司	400	0
三六零数字安全科技集团有限公司	375	375
深信服科技股份有限公司	328	0
新华三技术有限公司	318	0
北京天融信网络安全技术有限公司	150	0
远江盛邦（北京）网络安全科技股份有限公司	82	82
天津市国瑞数码安全系统股份有限公司	59	0
北京长亭科技有限公司	57	1
北京知道创宇信息技术有限公司	16	0
杭州迪普科技股份有限公司	14	0
京东科技信息技术有限公司	9	0
中国电信集团系统集成有限责任公司	4	4
北京知道创宇信息技	3	0

术股份有限公司		
北京信联数安科技有限公司	1	1
北京智游网安科技有限公司	1	1
深圳市腾讯计算机系统有限公司(玄武实验室)	1	1
内蒙古中叶信息技术有限责任公司	123	123
杭州美创科技有限公司	65	65
河南东方云盾信息技术有限公司	47	47
河南信安世纪科技有限公司	42	42
快页信息技术有限公司	24	24
奇安星城网络安全运营服务(长沙)有限公司	22	22
联想集团	20	20
安徽锋刃信息科技有限公司	18	18
杭州默安科技有限公司	11	11
重庆电信系统集成有限公司	11	11
内蒙古洞明科技有限公司	11	11
赛尔网络有限公司	7	7
广州安亿信软件科技有限公司	5	5
河南省鼎信信息安全等级测评有限公司	4	4

河北铸远网络科技有限公司	3	3
浙江木链物联网科技有限公司	3	3
江苏极元信息技术有限公司	3	3
宁夏凯信特信息科技有限公司	2	2
中能融合智慧科技有限公司	2	2
北京网御星云信息技术有限公司	2	2
西藏熙安信息技术有限责任公司	1	1
奇安信-工控安全实验室	1	1
德国电信咨询公司中国区公司	1	1
四川中成基业安全技术有限公司	1	1
南京师范大学常州创新发展研究院软件与信息安全测评中心	1	1
博智安全科技股份有限公司	1	1
郑州埃文科技	1	1
工业和信息化部电子第五研究所	1	1
北京山石网科信息技术有限公司	1	1
安徽长泰科技有限公司	1	1
重庆易阅科技有限公司	1	1
亚信科技(成都)有限	1	1

公司		
CNCERT 宁夏分中心	5	5
CNCERT 贵州分中心	4	4
个人	1051	1051
报送总计	9072	7156

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 475 个漏洞。WEB 应用 319 个，应用程序 65 个，网络设备（交换机、路由器等网络端设备）35 个，智能设备（物联网终端设备）34 个，操作系统 21 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	319
应用程序	65
网络设备（交换机、路由器等网络端设备）	35
智能设备（物联网终端设备）	34
操作系统	21
数据库	1

## 本周CNVD漏洞数量按影响类型分布

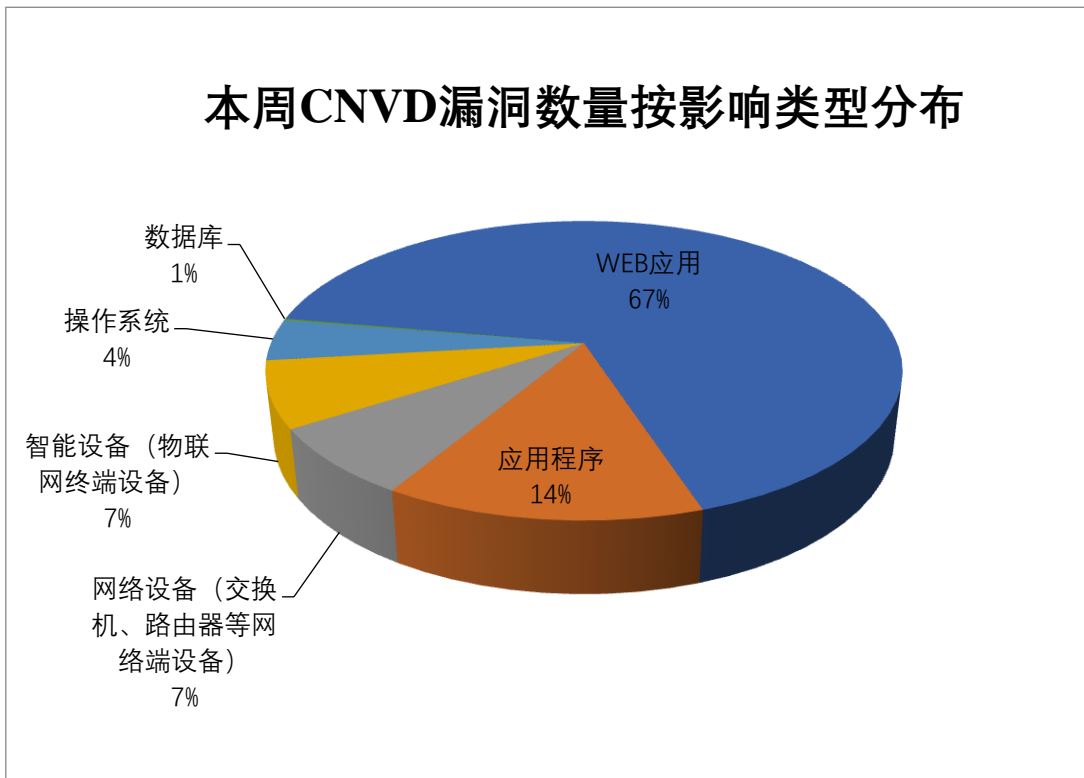


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Ricoh、Microsoft、Adobe 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	Ricoh	28	6%
2	Microsoft	19	4%
3	Adobe	13	3%
4	深圳市必联电子有限公司	10	2%
5	Google	9	2%
6	Linux	9	2%
7	D-Link	8	2%
8	杭州雄伟科技开发股份有限公司	6	1%
9	北京百卓网络技术有限公司	5	1%
10	其他	368	77%

### 本周行业漏洞收录情况

本周, CNVD 收录了 30 个电信行业漏洞, 31 个移动互联网行业漏洞(如下图所示)。其中, “NETGEAR R6250 缓冲区溢出漏洞、Lenovo XClarity Administrator 命令注入漏洞”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/>

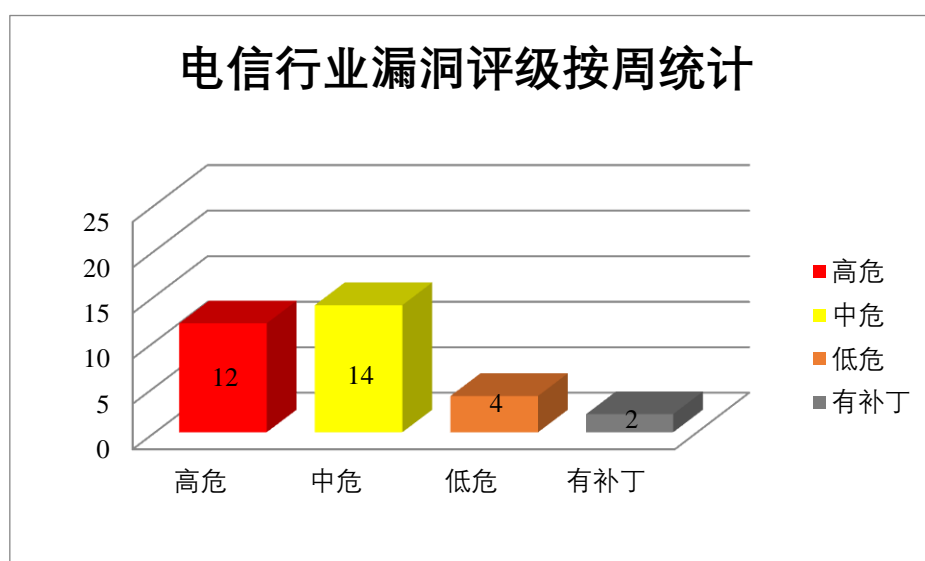


图 3 电信行业漏洞统计



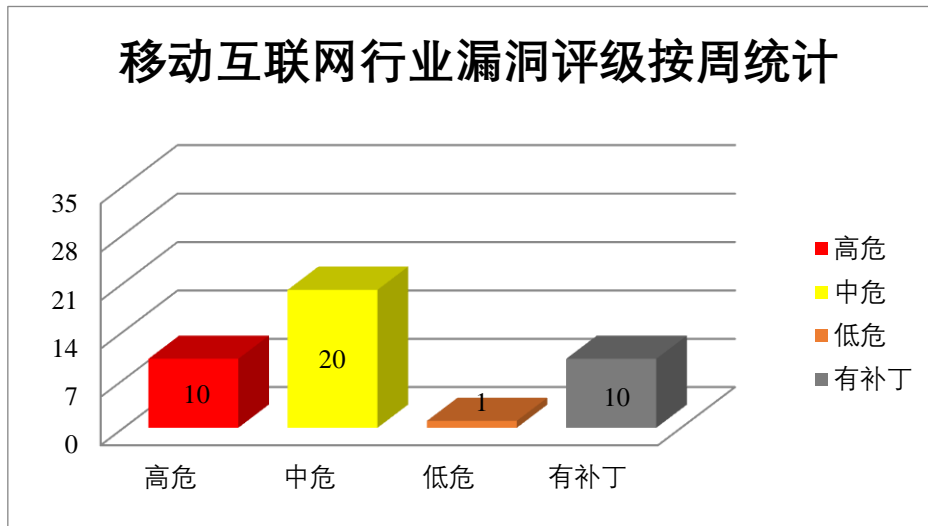


图 4 移动互联网行业漏洞统计

## 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、Google 产品安全漏洞

Google Android 是美国谷歌(Google)公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升，通过蓝牙远程执行代码等。

CNVD 收录的相关漏洞包括：Google Android 输入验证错误漏洞（CNVD-2023-53154、CNVD-2023-53156、CNVD-2023-53163）、Google Android 逻辑缺陷漏洞（CNVD-2023-53155）、Google Android 资源管理错误漏洞（CNVD-2023-53161、CNVD-2023-53160）、Google Android 加密问题漏洞（CNVD-2023-53159）、Google Android 代码问题漏洞（CNVD-2023-53158）。其中，“Google Android 资源管理错误漏洞（CNVD-2023-53160）、Google Android 加密问题漏洞（CNVD-2023-53159）”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-2023-53154>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53156>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53155>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53161>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53160>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53159>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53158>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53163>

## 2、Microsoft 产品安全漏洞

Microsoft SharePoint Server 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 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, 攻击者可利用漏洞进行欺骗攻击, 在系统上执行任意代码等。

CNVD 收录的相关漏洞包括: Microsoft SharePoint Server 欺骗漏洞 (CNVD-2023-53461、CNVD-2023-53462)、Microsoft Excel 远程代码执行漏洞 (CNVD-2023-53904、CNVD-2023-53906)、Microsoft Excel 安全功能绕过漏洞 (CNVD-2023-53907)、Microsoft Excel 代码执行漏洞 (CNVD-2023-53908、CNVD-2023-53909、CNVD-2023-53911)。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-2023-53461>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53462>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53904>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53906>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53907>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53908>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53909>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-53911>

## 3、Adobe 产品安全漏洞

Adobe Experience Manager (AEM) 是美国奥多比 (Adobe) 公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Animate 是美国奥多比 (Adobe) 公司的一套 Flash 动画制作软件。Adobe Substance 3D Designer 是美国奥多比 (Adobe) 公司的一款 3D 设计软件。Adobe Photoshop 是一个由 Adobe 开发和发行的应用软件, 用于图像处理。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞注入精心设计的有效载荷执行任意 Web 脚本或 HTML, 在系统上执行任意代码或者导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括: Adobe Experience Manager 跨站脚本漏洞 (CNVD-2023-54543)、Adobe Experience Manager 输入验证错误漏洞 (CNVD-2023-54542)、Adobe Animate 资源管理错误漏洞、Adobe Substance 3D Designer 缓冲区溢出漏洞、Adobe Animate 缓冲区溢出漏洞 (CNVD-2023-54550)、Adobe Photoshop 缓冲区溢出漏洞 (CNVD-2023-54549、CNVD-2023-54551)、Adobe Photoshop 资源管理错误漏洞 (CNVD-2023-54548)。其中, 除“Adobe Experience Manager 跨站脚本漏洞 (CNVD-2023-54543)、Adobe Experience Manager 输入验证错误漏洞 (CNVD-2023-54542)”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-2023-54543>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54542>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54545>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54544>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54550>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54549>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54548>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54551>

#### 4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致拒绝服务，提交特殊的请求，可以内核上下文执行任意代码，提升权限等。

CNVD 收录的相关漏洞包括：Linux kernel vidtv\_mux\_stop\_thread 拒绝服务漏洞、Linux kernel gsmdl\_write 拒绝服务漏洞、Linux Kernel 资源管理错误漏洞（CNVD-2023-54414）、Linux Kernel 缓冲区溢出漏洞（CNVD-2023-54413）、Linux Kernel RxRPC 竞争条件问题漏洞、Linux kernel 信息泄露漏洞（CNVD-2023-54416）、Linux kernel 拒绝服务漏洞（CNVD-2023-54415、CNVD-2023-54619）。其中，“Linux Kernel 拒绝服务漏洞（CNVD-2023-54619）”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-2023-54411>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54409>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54414>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54413>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54412>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54416>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54415>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54619>

#### 5、北京星网锐捷网络技术有限公司 RG-BCR860 操作系统命令注入漏洞

RG-BCR860 是中国锐捷网络（Ruijie Networks）公司的一款商业云路由器。本周，北京星网锐捷网络技术有限公司 RG-BCR860 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/sho>

[w/CNVD-2023-54867](https://www.cnvd.org.cn/entry/show/cnvd-2023-54867)

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: <https://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-2023-54439	HongCMS 跨站请求伪造漏洞 (CNVD-2023-54439)	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://github.com/Neeke/HongCMS/issues/13">https://github.com/Neeke/HongCMS/issues/13</a>
CNVD-2023-54442	Vim 缓冲区溢出漏洞 (CNVD-2023-54442)	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://github.com/vim/vim/issues/5041">https://github.com/vim/vim/issues/5041</a>
CNVD-2023-53465	Microsoft SharePoint 信息泄露漏洞 (CNVD-2023-53465)	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-2023-24954">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24954</a>
CNVD-2023-53467	Microsoft SharePoint Server 远程代码执行漏洞 (CNVD-2023-53467)	高	目前厂商已经发布了升级补丁以修复这个安全问题, 请到厂商的主页下载: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955</a>
CNVD-2023-53469	Microsoft SharePoint Server 远程代码执行漏洞 (CNVD-2023-53469)	高	目前厂商已经发布了升级补丁以修复这个安全问题, 请到厂商的主页下载: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744</a>
CNVD-2023-53471	Microsoft Windows Backup Engine 权限提升漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946</a>
CNVD-2023-54401	OpenCart SQL 注入漏洞 (CNVD-2023-54401)	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://github.com/opencart/opencart/issues/7612">https://github.com/opencart/opencart/issues/7612</a>
CNVD-2023-54400	PluckCMS 文件上传漏洞	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/pluck-cms/pluck/issues/79">https://github.com/pluck-cms/pluck/issues/79</a>
CNVD-2023-54437	PluckCMS 任意文件上传漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: <a href="https://github.com/pluck-cms/pluck/c">https://github.com/pluck-cms/pluck/c</a>

			ommit/be59bf6ba83bf41e9e91167e55330f56fcfb33c3
CNVD-2023-54440	EBCMS 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://github.com/a932278490/ebcms/issues/1">https://github.com/a932278490/ebcms/issues/1</a>

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升，通过蓝牙远程执行代码等。此外，Microsoft、Adobe、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，在系统上执行任意代码，提升权限等。另外，北京星网锐捷网络技术有限公司 RG-BCR860 操作系统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、novel-plus 文件上传漏洞

#### 验证描述

novel-plus（小说精品屋-plus）是一个多端（PC、WAP）阅读、功能完善的原创文学 CMS 系统。

novel-plus 存在文件上传漏洞，该漏洞源于/novel-admin/src/main/java/com/java2nb/common/controller/FileController.java 缺少对于文件上传的限制。攻击者可利用漏洞上传恶意 JSP 文件。

#### 验证信息

POC 链接：<https://github.com/201206030/novel-plus/issues/62>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2023-54404>

#### 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. IDC：2022 年中国云工作负载安全市场规模达 3.2 亿美元

本报告分别针对 2022 年中国公有云和私有云工作负载安全市场的规模、增长速度、

主要玩家、市场与技术的发展趋势等内容进行了详细研究。

参考链接：<https://www.secrss.com/articles/56393>

## 2. BlackByte 2.0 勒索软件：仅需 5 天即可渗透、加密和扩展

最近，微软的事件响应团队调查了 BlackByte 2.0 勒索软件攻击，并揭露了这些网络攻击的可怕速度和破坏性。

参考链接：<https://thehackernews.com/2023/07/blackbyte-20-ransomware-infiltrate.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](http://www.cert.org.cn)

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

电话：010-82991537