国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 03 月 13 日-2023 年 03 月 19 日 **2023 年第 11 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**高**。

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 301 个，其中高危漏洞 192 个、中危漏洞 98 个、低危漏洞 11 个。漏洞平均分值为 7.44。本周收录的漏洞中，涉及 0day 漏洞 179 个（占 59%），其中互联网上出现“JeeCMS 跨站脚本漏洞（CNVD-2023-17600）、WUZHI CMS 跨站脚本漏洞（CNVD-2023-17601）”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 30996 个，与上周（28859 个）环比增加 7%。

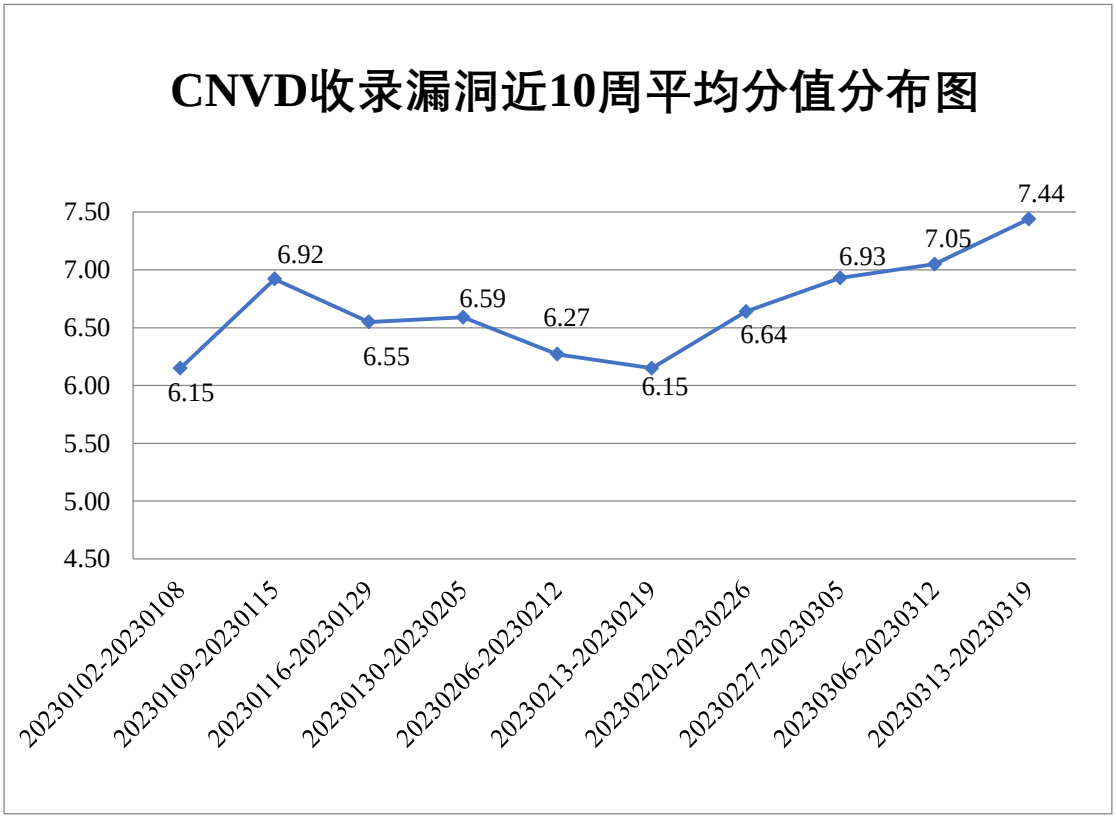

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 37 起，向基础电信企业通报漏洞事件 86 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 1407 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 338 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 57 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：

珠海国津软件科技有限公司、智恒科技股份有限公司、浙江禾连网络科技有限公司、浙江大华技术股份有限公司、云智慧（北京）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、新天科技股份有限公司、新浪网技术（中国）有限公司、西安九佳易信息资讯有限公司、武汉天地伟业科技有限公司、武汉慧谷通信技术有限公司、网宿科技股份有限公司、万商云集（成都）科技股份有限公司、同望科技股份有限公司、天维尔信息科技股份有限公司、泰华智慧产业集团股份有限公司、四川纵横六合科技股份有限公司、四川希望教育产业集团、神州数码控股有限公司、深圳市中电电力技术股份有限公司、深圳市长鑫盛通科技有限公司、深圳市万普拉斯科技有限公司、深圳市蓝凌软件股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市华远智能设备有限公司、深圳市合信自动化技术有限公司、深圳市共济科技股份有限公司、深圳市东宝信息技术有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海云赛智联信息科技有限公司、上海银狐科技有限公司、上海甲鼎信息技术有限公司、上海斐讯数据通信技术有限公司、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、上海爱数信息技术股份有限公司、熵基科技股份有限公司、厦门天锐科技股份有限公司、软通动力信息技术（集团）股份有限公司、全讯汇聚网络科技（北京）有限公司、鹏为软件股份有限公司、蓝鸽集团有限公司、开源字节、敬业钢铁有限公司、鲸充新能源科技有限公司、江苏紫清信息科技有限公司、江苏中天科技股份有限公司、江苏中天互联科技有限公司、江苏国光信息产业股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南创星科技股份有限公司、衡水金航计算机科技有限公司、河南云智互联科技有限公司、杭州雄伟科技开发股份有限公司、杭州图特信息科技有限公司、杭州平治科技、杭州领悟网络科技有限公司、杭州海康威视数字技术股份有限公司、哈尔滨伟成科技有限公司、广州红帆科技有限公司、广州达梦网络科技有限公司、广东保伦电子股份有限公司、仿脑科技（深圳）有限公司、东北师大理想软件股份有限公司、畅捷通信息技术股份有限公司、北京中创视讯科技有限公司、北京云畅观复软件技术有限公司、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、北京小米科技有限责任公司、北京五指互联科技有限公司、北京网瑞达科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京数字政通科技股份有限公司、北京清流技术股份有限公司、北京欧倍尔软件技术开发有限公司、北京九思协同软件有限公司、北京后盾计算机技术培训有限责任公司、安徽省科迅教育装备有限公司、WAVLINK 和《中国医药报》社有限公司。

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、新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、上海齐同信息科技有限公司、北京升鑫网络科技有限公司、北京山石网科信息技术有限公司、山东鼎夏智能科技有限公司、杭州默安科技有限公司、浙江安腾信息技术有限公司、安徽锋刃信息科技有限公司、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、奇安星城网络安全运营服务（长沙）有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、江苏君立华域信息安全技术股份有限公司、上海纽盾科技股份有限公司、快页信息技术有限公司、杭州美创科技有限公司、网驰数字科技（山东）有限公司、广州安海信息安全技术有限公司、河南灵创电子科技有限公司、中国工商银行、北京远禾科技有限公司、重庆易阅科技有限公司、郑州埃文科技、江苏晟晖信息科技有限公司、工业和信息化部电子第五研究所、北京安帝科技有限公司、北京众安天下科技有限公司、广东唯顶信息科技股份有限公司、合肥梆梆信息科技有限公司、山东云天安全技术有限公司、湖南轻山信息技术有限公司、苏州棱镜七彩信息科技有限公司、赛尔网络有限公司、宁夏凯信特信息科技有限公司、北方实验室（沈阳）股份有限公司、浙江大学控制科学与工程学院、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 30966 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）、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 29264 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）	25614	25614
三六零数字安全科技集团有限公司	1718	1718
奇安信网神（补天平台）	1109	1109
北京启明星辰信息安	866	11

全技术有限公司		
上海交大	823	823
新华三技术有限公司	677	0
深信服科技股份有限公司	428	0
安天科技集团股份有限公司	234	1
北京神州绿盟科技有限公司	177	0
北京天融信网络安全技术有限公司	137	12
阿里云计算有限公司	127	4
北京数字观星科技有限公司	95	0
恒安嘉新（北京）科技股份公司	70	0
杭州安恒信息技术股份有限公司	59	59
京东科技信息技术有限公司	43	7
中国电信集团系统集成有限责任公司	30	0
南京众智维信息科技有限公司	17	17
北京知道创宇信息技术有限公司	1	0
西安四叶草信息技术有限公司	1	1
北京华顺信安信息技术有限公司	411	0
上海齐同信息科技有限公司	85	85
北京升鑫网络科技有限公司	52	52
北京山石网科信息技	48	48

术有限公司		
山东鼎夏智能科技有限公司	36	36
杭州默安科技有限公司	23	23
浙江安腾信息技术有限公司	21	21
安徽锋刃信息科技有限公司	20	20
博智安全科技股份有限公司	19	19
河南东方云盾信息技术有限公司	15	15
奇安星城网络安全运营服务（长沙）有限公司	8	8
北京云科安信科技有限公司（Seraph 安全实验室）	8	8
江苏君立华域信息安全技术股份有限公司	7	7
上海纽盾科技股份有限公司	7	7
西门子（中国）有限公司	7	0
快页信息技术有限公司	6	6
杭州美创科技有限公司	6	6
网驰数字科技（山东）有限公司	6	6
广州安海信息安全技术有限公司	3	3
河南灵创电子科技有限公司	3	3

中国工商银行	3	3
北京远禾科技有限公司	3	3
重庆易阅科技有限公司	2	2
郑州埃文科技	2	2
江苏晟晖信息科技有限公司	2	2
工业和信息化部电子第五研究所	2	2
北京安帝科技有限公司	2	2
北京众安天下科技有限公司	1	1
广东唯顶信息科技股份有限公司	1	1
合肥梆梆信息科技有限公司	1	1
山东云天安全技术有限公司	1	1
湖南轻山信息技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
赛尔网络有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
浙江大学控制科学与工程学院	1	1
亚信科技（成都）有限公司	1	0
任子行网络技术股份有限公司	1	1

CNCERT 宁夏分中心	5	5
CNCERT 广西分中心	2	2
CNCERT 贵州分中心	1	1
个人	1182	1182
报送总计	34235	30966

本周漏洞按类型和厂商统计

本周，CNVD 收录了 301 个漏洞。WEB 应用 122 个，网络设备（交换机、路由器等网络端设备）109 个，应用程序 60 个，智能设备 8 个，数据库 1 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	122
网络设备（交换机、路由器等网络端设备）	109
应用程序	60
智能设备	8
数据库	1
安全产品	1

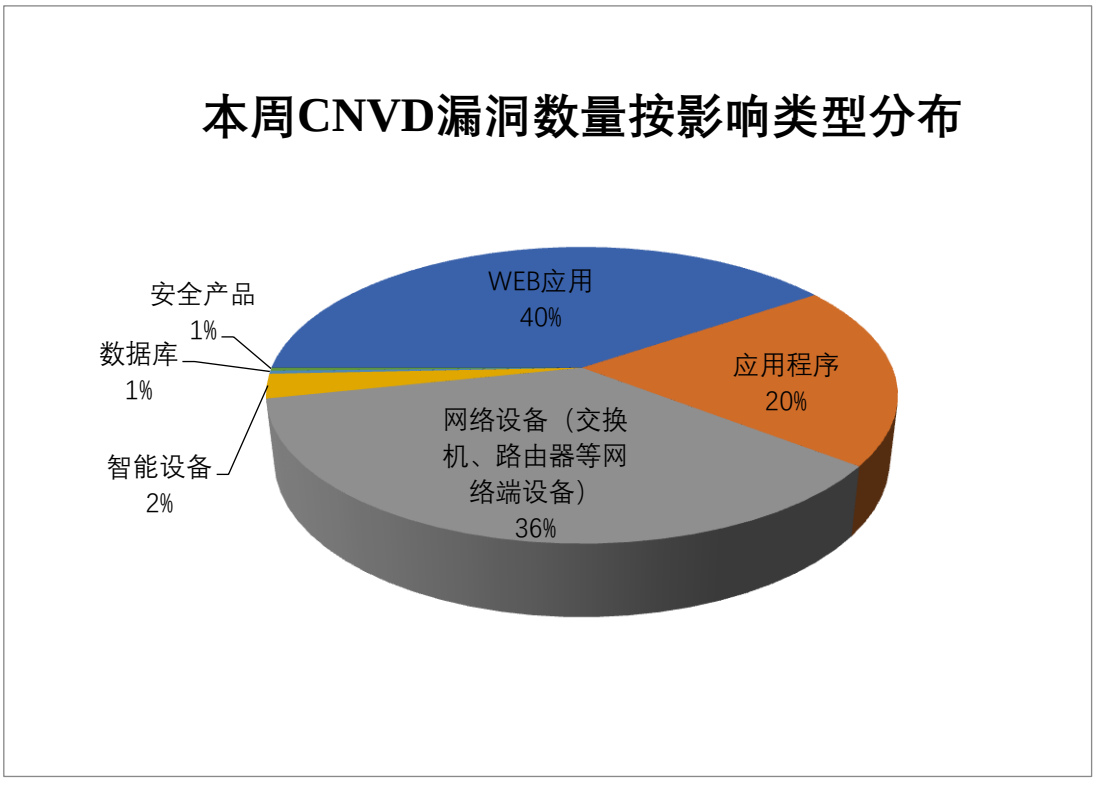

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siretta、D-Link、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	Siretta	57	19%
2	D-Link	23	8%
3	Adobe	10	3%
4	Mozilla	10	3%
5	Advantech	10	3%
6	Google	8	3%
7	Siemens	7	2%
8	Beauty Parlour Management System	5	2%
9	TOTOLINK	5	2%
10	其他	166	55%

本周行业漏洞收录情况

本周，CNVD 收录了 95 个电信行业漏洞，16 个移动互联网行业漏洞，65 个工控行业漏洞（如下图所示）。其中，“TP-Link Archer AX21 AX1800 命令注入漏洞、Siretta QUARTZ-GOLD 缓冲区溢出漏洞（CNVD-2023-16876）”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/

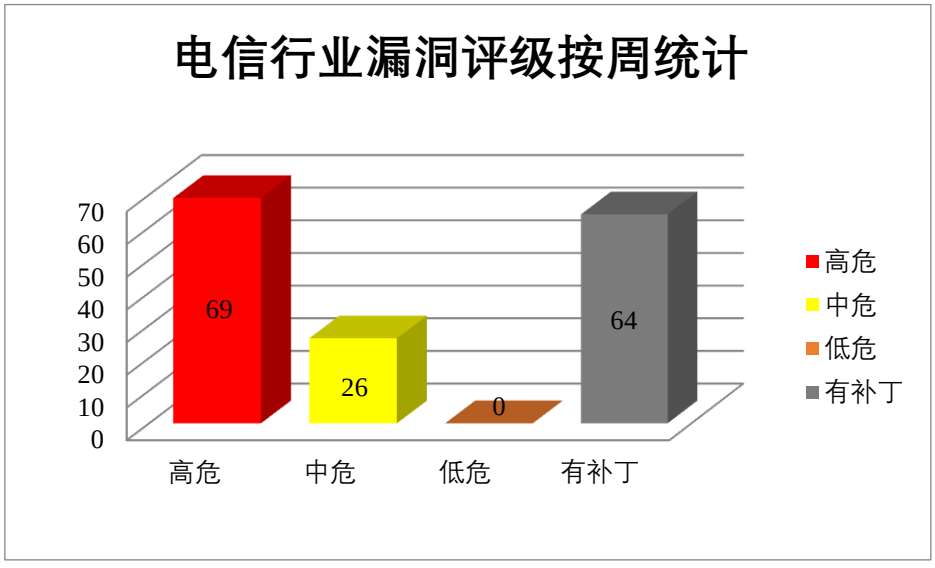

图 3 电信行业漏洞统计

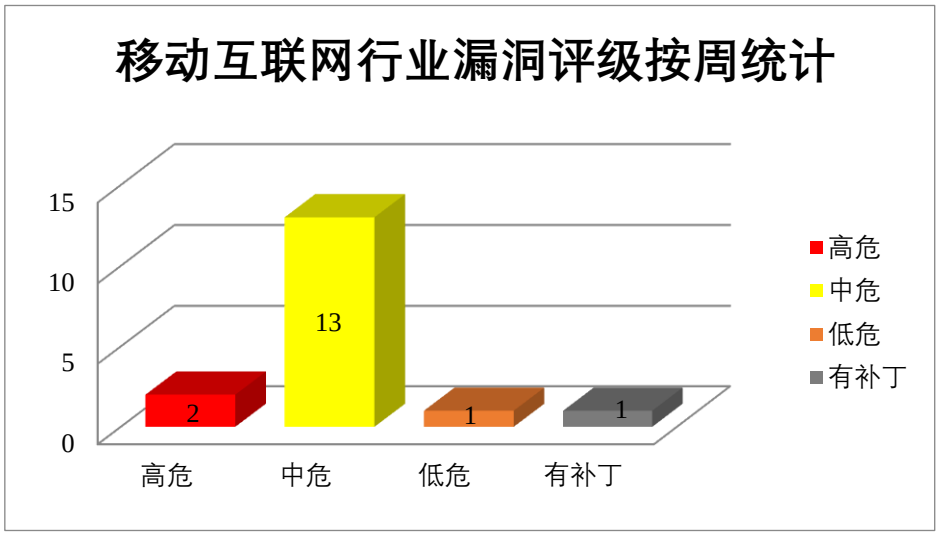

图 4 移动互联网行业漏洞统计

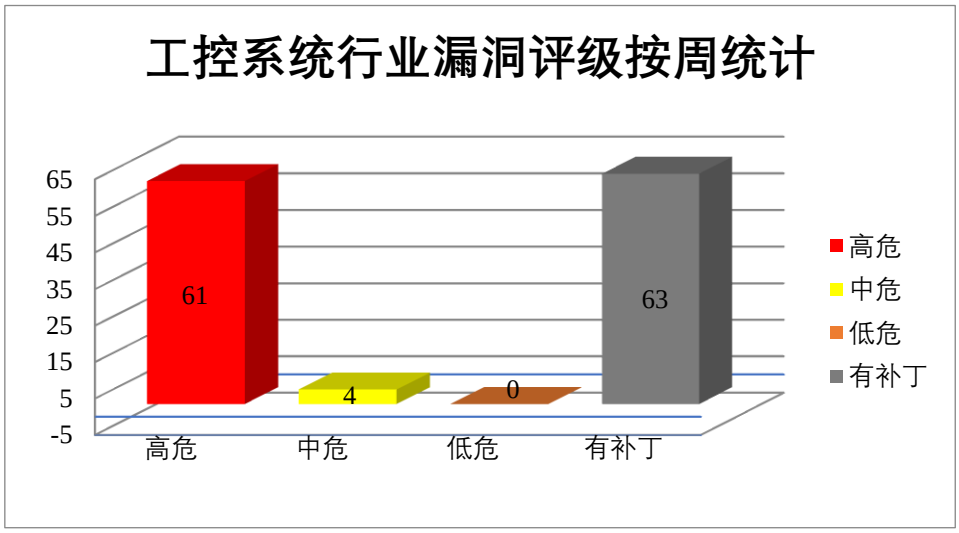

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，通过特制的 HTML 页面导致堆损坏等。

CNVD 收录的相关漏洞包括：Google Chrome DevTools 组件类型混肴漏洞、Google Chrome Crash reporting 组件缓冲区溢出漏洞、Google Chrome Core 资源管理错误漏洞、Google Chrome Autofill 组件代码问题漏洞、Google Chrome V8 类型混淆漏洞（CNVD-2023-17527）、Google Chrome UMA 组件缓冲区溢出漏洞（CNVD-2023-17526）、Google Chrome DevTools 资源管理错误漏洞（CNVD-2023-17525）、Google Chrome

Web Audio API 组件缓冲区溢出漏洞。其中，除“Google Chrome Autofill 组件代码问题漏洞”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-2023-17524
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17523
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17522
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17521
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17527
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17526
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17525
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17528

2、D-Link 产品安全漏洞

D-Link DIR-605L 是中国 D-Link 公司的一款无线路由器。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致远程代码执行或服务中断。

CNVD 收录的相关漏洞包括：D-Link DIR-605L 缓冲区溢出漏洞（CNVD-2023-17668、CNVD-2023-17667、CNVD-2023-17666、CNVD-2023-17670、CNVD-2023-17669、CNVD-2023-17673、CNVD-2023-17672、CNVD-2023-17671）。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-2023-17668
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17667
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17666
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17670
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17669
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17673
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17672
https://www.cnvd.org.cn/flaw/show/CNVD-2023-17671

3、Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe Premiere Rush 是美国奥多比（Adobe）公司的一套跨平台的视频编辑软件。Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致敏感内存泄露，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Bridge 堆缓冲区溢出漏洞（CNVD-2023-17020、CNVD-2023-17019）、Adobe Bridge 越界读取漏洞（CNVD-2023-17018）、Adobe Photoshop 输入验证错误漏洞（CNVD-2023-17021）、Adobe Photoshop 越界写入漏洞（CNVD-2023-17022）、Adobe Premiere Rush 堆栈缓冲区溢出漏洞、Adobe After Effects 越界读取漏洞（CNVD-2023-17024）、Adobe Animate 内存错误引用漏洞。除“Adobe Bridge 越界读取漏洞（CNVD-2023-17018）、Adobe After Effects 越界读取漏洞（CNVD-2023-17024）”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-2023-17020

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17019

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17018

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17021

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17022

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17023

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17024

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17047

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 PollBot 是 Mozilla 基金会的一个微服务。将人类从 Firefox 发布过程中的状态轮询这一繁重任务中解放出来。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将任何人重定向到恶意站点，绕过已实施的安全限制在受害者的浏览器中执行任意 JavaScript 代码，通过使程序在当前目录中搜索系统库提升权限等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 竞争条件问题漏洞（CNVD-2023-17319）、Mozilla Firefox 权限提升漏洞（CNVD-2023-17318）、Mozilla PollBot 开放重定向漏洞、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-17321、CNVD-2023-17323）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-17324）、Mozilla Firefox 安全特征问题漏洞（CNVD-2023-17322、CNVD-2023-17320）。其中，除“Mozilla Firefox 权限提升漏洞（CNVD-2023-17318）、Mozilla PollBot 开放重定向漏洞”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-2023-17319

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17318

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17317

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17321

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17320

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17324

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17323

https://www.cnvd.org.cn/flaw/show/CNVD-2023-17322

5、 Advantech iView SQL 注入漏洞（CNVD-2023-16475）

Advantech iView 是中国 Advantech 公司的一个基于简单网络协议（SNMP）来对 B + B SmartWorx 设备进行管理的软件。本周，Advantech iView 5.7.04.6469 之前版本被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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-2023-16475

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-2023-16471	Advantech R-SeeNet 堆栈缓冲区溢出漏洞（CNVD-2023-16471）	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：https://www.cisa.gov/uscert/ics/advisories/icsa-22-291-01
CNVD-2023-16470	Advantech R-SeeNet 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，补丁获取链接：https://www.cisa.gov/uscert/ics/advisories/icsa-22-291-01
CNVD-2023-16473	Advantech iView SQL 注入漏洞（CNVD-2023-16473）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.tw/support/details/firmware?id=1-HIPU-183
CNVD-2023-16472	Advantech iView SQL 注入漏洞（CNVD-2023-16472）	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://www.advantech.com/
CNVD-2023-16476	Advantech iView 访问控制错误漏洞（CNVD-2023-16476）	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://www.advantech.com/
CNVD-2023-16478	Advantech iView 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/
CNVD-2023-16477	Advantech iView 命令注入漏洞（CNVD-2023-16477）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/
CNVD-2023-16877	Siretta QUARTZ-GOLD 缓冲区溢出漏洞（CNVD-2023-16	高	厂商已发布了漏洞修复程序，请及时关注更新：

	877）		https://www.siretta.com/products/industrial-routers/4g-lte-router/gigabit-ethernet-small-footprint-lte-router-eu/
CNVD-2023-16880	Siretta QUARTZ-GOLD 缓冲区溢出漏洞（CNVD-2023-16880）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.siretta.com/products/industrial-routers/4g-lte-router/gigabit-ethernet-small-footprint-lte-router-eu/
CNVD-2023-16878	Siretta QUARTZ-GOLD 缓冲区溢出漏洞（CNVD-2023-16878）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.siretta.com/products/industrial-routers/4g-lte-router/gigabit-ethernet-small-footprint-lte-router-eu/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，通过特制的 HTML 页面导致堆损坏等等。此外，D-Link、Adobe、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致远程代码执行或服务中断，将任何人重定向到恶意站点，绕过已实施的安全限制在受害者的浏览器中执行任意 JavaScript 代码，通过使程序在当前目录中搜索系统库提升权限。另外，Advantech iView 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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、JeeCMS 跨站脚本漏洞（CNVD-2023-17600）

验证描述

Jeecms 是中国金磊科技发展（Jeecms）公司的一套使用 Java 语言开发的内容管理系统（CMS）。

JeeCMS 1.0.1 版本存在跨站脚本漏洞。攻击者可利用该漏洞通过 commentText 参数中特制的负载执行任意的 web 脚本或 HTML。

验证信息

POC 链接：https://github.com/blackjliuyun/cvetest/issues/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-17600

信息提供者

北京神州绿盟科技有限公司

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. 微软释出更新修复两个正被利用的 0day

微软释出了三月例行安全更新，修复了 74 个漏洞，其中两个是正被利用的 0day——CVE-2023-23397 的危险得分 9.8/10，是 Microsoft Outlook 中的一个提权漏洞。

参考链接：https://www.solidot.org/story?sid=74412

2. 工信部立即查处“3·15”晚会曝光的破解版 App 违法违规收集用户个人信息行为

据工业和信息化部官微“工信微报”消息，针对“3·15”晚会报道的部分破解版 App 违法违规收集用户个人信息问题，立即组织核查，并依据《个人信息保护法》《电信和互联网用户个人信息保护规定》等有关法律法规要求进行严厉查处。

参考链接：https://www.ithome.com/0/680/152.htm

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