国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 06 月 12 日-2023 年 06 月 18 日 **2023 年第 24 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 511 个，其中高危漏洞 268 个、中危漏洞 214 个、低危漏洞 29 个。漏洞平均分值为 6.65。本周收录的漏洞中，涉及 0day 漏洞 420 个（占 82%），其中互联网上出现“Online Exam System Master.php 文件 SQL 注入漏洞、Judging Management System SQL 注入漏洞（CNVD-2023-48485）”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 14881 个，与上周（27201 个）环比减少 45%。

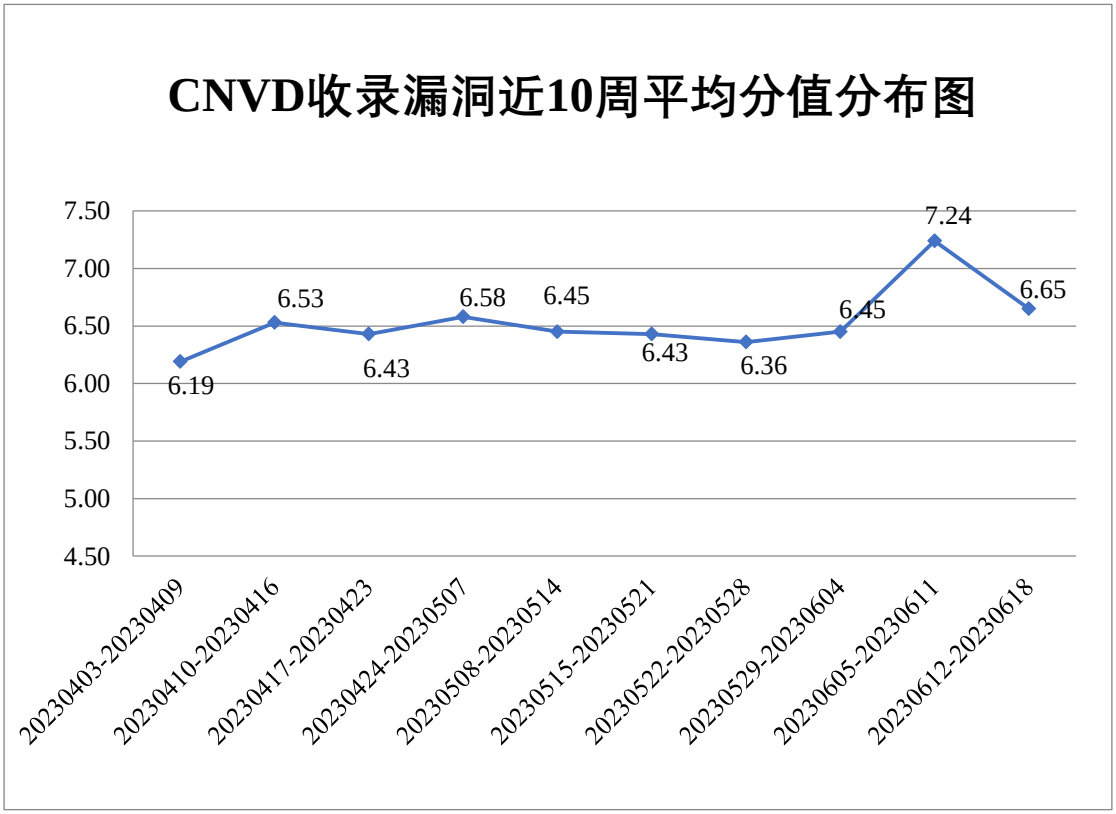

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电信企业通报漏洞事件 15 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 1121 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 250 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 51 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：

珠海奔图打印科技有限公司、中山市岩峰照明科技有限公司、中青益信（杭州）科技有限公司、中科医创科技有限公司、中国计算机世界出版服务公司、浙江莲芯健康管理有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、新印科技股份有限公司、新天科技股份有限公司、新都（青岛）办公设备有限公司、象智科技（武汉）有限公司、西安众邦网络科技有限公司、西安沃户时间区块链科技股份有限公司、西安建大静态交通研究院有限公司、武汉城投停车场投资建设管理有限公司、无锡信捷电气股份有限公司、温州市万旗信息科技有限公司、威海市天罡仪表股份有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天津天堰科技股份有限公司、天津市医学堂科技有限公司、泰华智慧产业集团股份有限公司、宿迁鑫潮信息技术有限公司、苏州天一信德环保科技有限公司、苏州思迪信息技术有限公司、四川众望升腾科技有限公司、神州锐达（北京）科技股份公司、深圳甜糖科技有限公司、深圳市同为数码科技股份有限公司、深圳市松洋健康管理有限公司、深圳市明源云科技有限公司、深圳市锟铻科技有限公司、深圳市金版文化数字传媒有限公司、深圳市捷顺科技实业股份有限公司、深圳市航通北斗信息技术有限公司、深圳市广道数字技术股份有限公司、深圳市迪博企业风险管理技术有限公司、深圳市大白菜科技有限公司、深圳市必联电子有限公司、上海挚达科技发展股份有限公司、上海优尔蓝信息科技有限公司、上海宜同贸易有限公司、上海新朋程数据科技发展有限公司、上海威派格环保科技有限公司、上海绮梦网络科技有限公司、上海凯京信达科技集团有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海朝明教育科技有限公司、熵基科技股份有限公司、山东博硕自动化技术有限公司、山东爱尚家网络有限公司、厦门游奕网络科技有限公司、厦门四信通信科技有限公司、瑞纳智能设备股份有限公司、普联技术有限公司、鹏为软件股份有限公司、南京苏文软件技术有限公司、南京品德科技有限责任公司、南京纳龙科技有限公司、摩莎科技（上海）有限公司、蜜雪冰城股份有限公司、梅州市青云客网络科技有限公司、理光（中国）投资有限公司、雷神（武汉）网络技术有限公司、金卡银证软件（杭州）有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、江苏兰德数码科技有限公司、江苏金智教育信息股

份有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、汇鼎数据科技（上海）有限公司、湖南快乐车行露营地投资发展有限公司、洪湖尔创网联信息技术有限公司、合肥天寻信息科技有限公司、杭州思福迪信息技术有限公司、杭州巨星科技股份有限公司、杭州海康威视数字技术股份有限公司、杭州博联智能科技股份有限公司、海鸿达（北京）餐饮管理有限公司、哈尔滨新中新电子股份有限公司、哈尔滨伟成科技有限公司、国泰新点软件股份有限公司、广州易凯软件技术有限公司、广州思迈特软件有限公司、广州市凝智科技有限公司、广州南方卫星导航仪器有限公司、广州龙建达电子股份有限公司、广州鸿根信息科技有限公司、广联达科技股份有限公司、广东小天才科技有限公司、瓜子汽车服务（天津）有限公司、福州网钛软件科技有限公司、福建平潭海峡中药材交易有限责任公司、东华医为科技有限公司、帝国软件、创维集团有限公司、传新科技有限公司、成都市灵奇空间软件有限公司、成都生动网络科技有限公司、北京卓众出版有限公司、北京元年科技股份有限公司、北京用友政务软件股份有限公司、北京易酒批电子商务有限公司、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、北京网康科技有限公司、北京通达信科科技有限公司、北京巧巧时代网络科技有限公司、北京力控元通科技有限公司、北京朗新天霁软件技术有限公司、北京京顺医院有限公司、北京金和网络股份有限公司、北京简网世纪科技有限公司、北京宏景世纪软件股份有限公司、北京东大正保科技有限公司、北京点为信息科技有限公司、北京创今世纪科技有限公司、北京必迈体育用品有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安徽中技国医医疗科技有限公司、安徽青柿信息科技有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心、Z 平台、WAVLINK、SEACMS、Jfinal cms、DWSurvey 调问和 Dreamer CMS。

本周，CNVD 发布了《Microsoft 发布 2023 年 6 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8931

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。快页信息技术有限公司、内蒙古中叶信息技术有限责任公司、河南东方云盾信息技术有限公司、杭州美创科技有限公司、安徽锋刃信息科技有限公司、博智安全科技股份有限公司、奇安星城网络安全运营服务（长沙）有限公司、联想集团、重庆电信系统集成公司、北京众安天下科技有限公司、河南信安世纪科技有限公司、赛尔网络有限公司、贵州多彩网安科技有限公司、广州安亿信

软件科技有限公司、河北镌远网络科技有限公司、郑州埃文科技、河南省鼎信信息安全等级测评有限公司、浙江木链物联网科技有限公司、重庆易阅科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、江苏天竞云合数据技术有限公司、北京水木羽林科技有限公司及其他个人白帽子向 CNVD 提交了 14881 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 13442 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）	10778	10778
上海交大	917	917
斗象科技（漏洞盒子）	904	904
三六零数字安全科技集团有限公司	843	843
北京启明星辰信息安全技术有限公司	651	0
新华三技术有限公司	531	0
深信服科技股份有限公司	397	8
安天科技集团股份有限公司	395	0
北京神州绿盟科技有限公司	289	0
北京天融信网络安全技术有限公司	202	0
北京数字观星科技有限公司	152	0
北京长亭科技有限公司	145	0
远江盛邦（北京）网络安全科技股份有限公司	82	82
京东科技信息技术有限公司	18	0
杭州迪普科技股份有	13	0

限公司		
卫士通信息产业股份有限公司	6	6
南京众智维信息科技有限公司	6	6
阿里云计算有限公司	4	4
北京知道创宇信息技术有限公司	2	0
北京智游网安科技有限公司	1	1
快页信息技术有限公司	100	100
内蒙古中叶信息技术有限责任公司	57	57
河南东方云盾信息技术有限公司	54	54
杭州美创科技有限公司	48	48
安徽锋刃信息科技有限公司	27	27
博智安全科技股份有限公司	25	25
西门子（中国）有限公司	15	0
奇安星城网络安全运营服务（长沙）有限公司	12	12
联想集团	11	11
重庆电信系统集成公司	9	9
北京众安天下科技有限公司	7	7
河南信安世纪科技有限公司	5	5
赛尔网络有限公司	4	4

贵州多彩网安科技有限公司	4	4
广州安亿信软件科技有限公司	3	3
河北镌远网络科技有限公司	2	2
郑州埃文科技	2	2
河南省鼎信信息安全等级测评有限公司	2	2
浙江木链物联网科技有限公司	1	1
重庆易阅科技有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
江苏天竞云合数据技术有限公司	1	1
北京水木羽林科技有限公司	1	1
个人	955	955
报送总计	17683	14881

本周漏洞按类型和厂商统计

本周，CNVD 收录了 511 个漏洞。WEB 应用 298 个，网络设备（交换机、路由器等网络端设备）109 个，应用程序 67 个，操作系统 26 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	298
网络设备（交换机、路由器等网络端设备）	109
应用程序	67
操作系统	26
智能设备（物联网终端设备）	6

安全产品	5

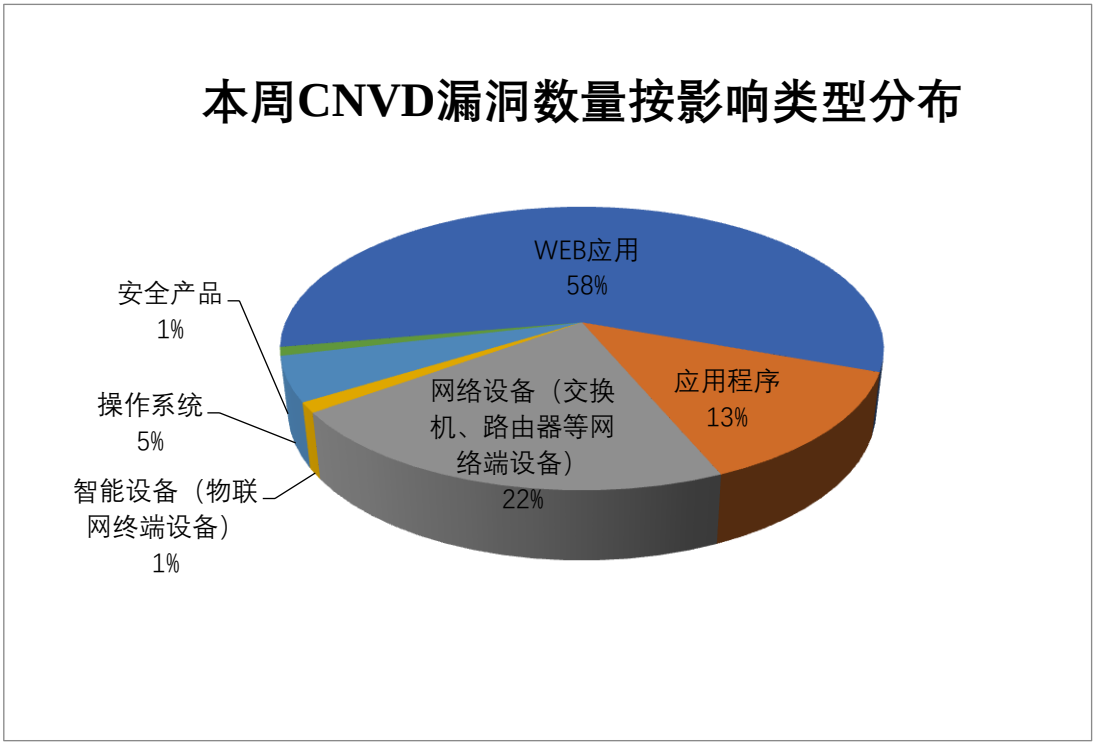

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及新华三技术有限公司、Google、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	新华三技术有限公司	20	4%
2	Google	19	4%
3	Adobe	19	4%
4	Siemens	15	3%
5	TP-LINK	14	3%
6	北京网康科技有限公司	13	2%
7	Linux	10	2%
8	睿因科技（深圳）有限公司	10	2%
9	上海艾泰科技有限公司	9	2%
10	其他	382	74%

本周行业漏洞收录情况

本周，CNVD 收录了 70 个电信行业漏洞，24 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“ISC BIND 缓冲区溢出漏洞、Siemens SIMATIC STE

P 7 V5 远程代码执行漏洞”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/

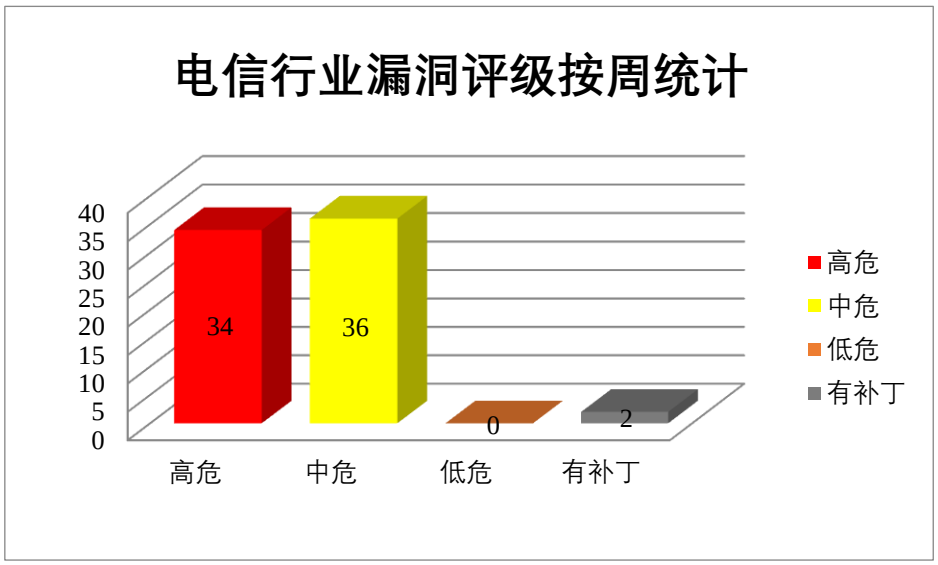

图 3 电信行业漏洞统计

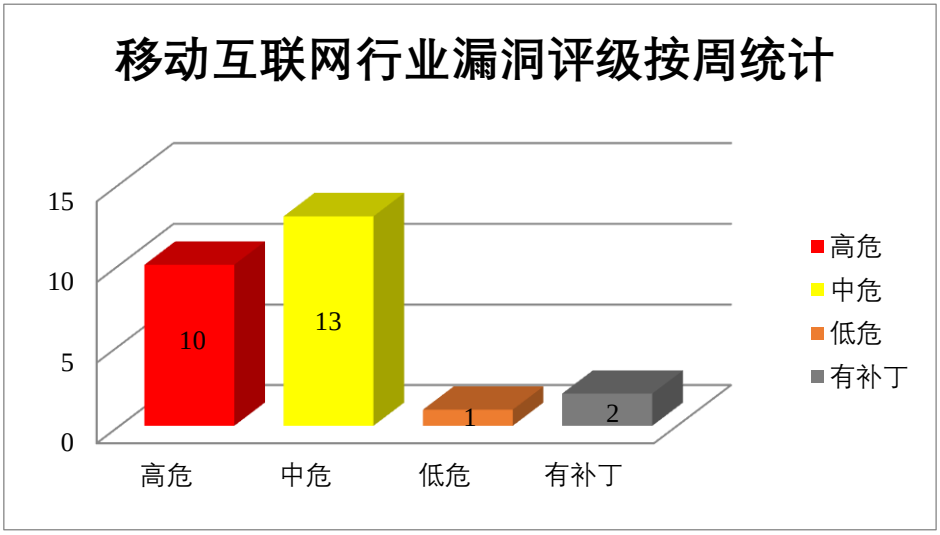

图 4 移动互联网行业漏洞统计

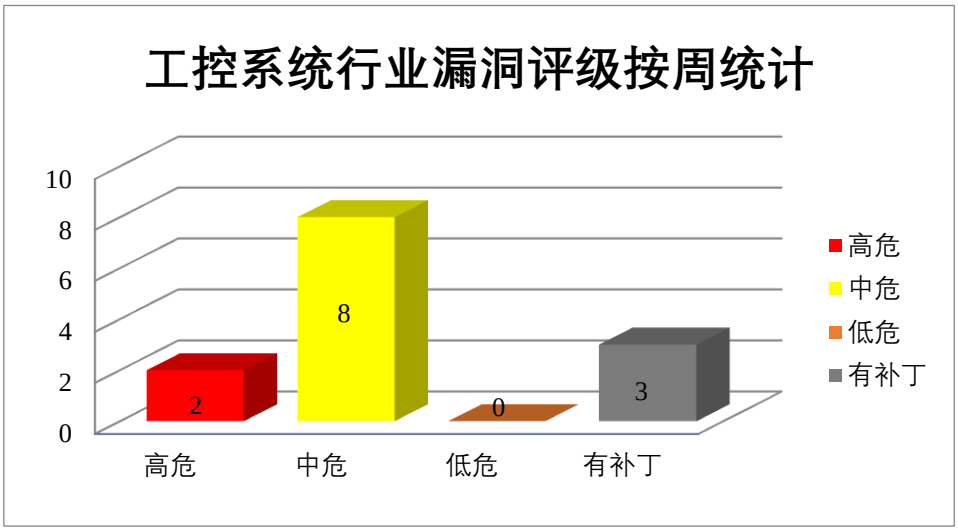

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞在系统上执行任意代码或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome 类型混肴漏洞、Google Chrome Extensions 组件内存错误引用漏洞、Google Chrome PDF 组件内存错误引用漏洞（CNVD-2023-46113、CNVD-2023-46115、CNVD-2023-46110）、Google Chrome V8 组件代码执行漏洞（CNVD-2023-46117、CNVD-2023-46116）、Google Chrome Mojo 组件代码执行漏洞。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-2023-46107

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46110

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46109

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46113

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46117

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46116

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46115

https://www.cnvd.org.cn/flaw/show/CNVD-2023-46119

2、 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，攻击者可利用漏洞在未经授权的情况下执行管理命令，导

致用户崩溃或提升系统权限等。

CNVD 收录的相关漏洞包括：Linux kernel 命令执行漏洞、Linux kernel ntfs_set_ea 越界读取漏洞、Linux kernel 缓冲区溢出漏洞（CNVD-2023-48543）、Linux kernel 资源管理错误漏洞（CNVD-2023-48542、CNVD-2023-48540、CNVD-2023-48546、CNVD-2023-48545）、Linux kernel 数字错误漏洞（CNVD-2023-48544）。其中，“Linux kernel 资源管理错误漏洞（CNVD-2023-48542、CNVD-2023-48540）”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-2023-48539
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48537
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48543
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48542
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48540
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48546
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48545
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48544

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。本周，上述产品被披露存在 URL 重定向漏洞，攻击者可利用漏洞将用户重定向到恶意网站。

CNVD 收录的相关漏洞包括：Adobe Experience Manager URL 重定向漏洞（CNVD-2023-45904、CNVD-2023-45903、CNVD-2023-45901、CNVD-2023-45906、CNVD-2023-45905、CNVD-2023-45909、CNVD-2023-45908、CNVD-2023-45907）。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-2023-45904
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45903
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45901
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45906
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45905
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45909
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45908
https://www.cnvd.org.cn/flaw/show/CNVD-2023-45907

4、 Juniper Networks 产品安全漏洞

Juniper Networks Junos OS 是美国瞻博网络（Juniper Networks）公司的一套专用于该公司的硬件设备的网络操作系统。该操作系统提供了安全编程接口和 Junos SDK。Juniper Networks Junos OS Evolved 是美国瞻博网络（Juniper Networks）公司的 Junos OS 的升级版系统。Juniper Networks Paragon Active Assurance 是美国瞻博网络（Juniper Networks）公司的一种可编程的测试和服务保证解决方案。使用基于软件和流量生成的测试代理，可作为 SaaS 解决方案从云中轻松使用和交付，或在 NFV 环境中本地部署。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控制台访问控制，将潜在的恶意文件复制到本地系统上的现有 Docker 容器中，随后管理员可能会无意中启动 Docker 容器，导致恶意文件以 root 身份执行等。

CNVD 收录的相关漏洞包括：Juniper Networks Junos OS 访问控制错误漏洞（CNVD-2023-48478）、Juniper Networks Junos OS Evolved 权限提升漏洞、Juniper Networks Junos OS 资源管理错误漏洞（CNVD-2023-48482、CNVD-2023-49464）、Juniper Networks Junos OS 输入验证错误漏洞（CNVD-2023-48481）、Juniper Networks Junos OS 拒绝服务漏洞（CNVD-2023-49463）、Juniper Networks Junos OS bbe-smgd 拒绝服务漏洞、Juniper Networks Paragon Active Assurance 跨站脚本漏洞。其中，“Juniper Networks Junos OS 访问控制错误漏洞（CNVD-2023-48478）、Juniper Networks Paragon Active Assurance 跨站脚本漏洞”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-2023-48478
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48477
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48482
https://www.cnvd.org.cn/flaw/show/CNVD-2023-48481
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49463
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49462
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49465
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49464

5、TP-Link Archer VR1600V 命令注入漏洞

TP-Link Archer VR1600V 是中国普联（TP-LINK）公司的一款无线调制解调器。本周，TP-Link Archer VR1600V 被披露存在命令注入漏洞。攻击者可利用该漏洞以管理员用户身份通过“X_TP_IfName”参数打开操作系统级 shell。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-2023-49482

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-2023-46120	Google Chrome Swiftshader 组件越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_30.html
CNVD-2023-46121	WordPress Easy Google Maps plugin 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/google-maps-easy/
CNVD-2023-46125	Google Chrome 代码执行漏洞（CNVD-2023-46125）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_16.html
CNVD-2023-46127	Google Chrome on Chrome OS 内存错误引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-chromeos.html
CNVD-2023-46128	Google Chrome on Chrome OS 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-chromeos.html
CNVD-2023-48548	Siemens SIMATIC STEP 7 V5 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-968170.html
CNVD-2023-48547	Siemens Mendix SAML 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-851884.html
CNVD-2023-48555	Siemens Teamcenter Visualization and JT2Go 内存损坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-538795.html
CNVD-2023-48554	Siemens SICAM A8000 Devices CPCI85 Firmware 硬编码凭证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-731916.html

CNVD-2023-48553	Siemens SICAM A8000 Devices CPCI85 Firmware 硬编码凭证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-731916.html

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码或导致应用程序崩溃。此外，Linux、Adobe、Juniper Networks 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在未经授权的情况下执行管理命令，导致用户崩溃或提升系统权限等。另外，TP-Link Archer VR1600V 被披露存在命令注入漏洞。攻击者可利用该漏洞以管理员用户身份通过“X_TP_IfName”参数打开操作系统级 shell。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 Exam System Master.php 文件 SQL 注入漏洞

验证描述

Online Exam System 是一个在线考试系统。

Online Exam System v1.0 版本存在 SQL 注入漏洞，该漏洞源于/classes/Master.php?f=delete_service/kelasdosen/data 的参数 columns、data 缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/tht1997/CVE_2023/blob/main/online_exam/kelasdosen.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-48484

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. Android GravityRAT 恶意软件可窃取 WhatsApp 备份

自 2022 年 8 月以来，一场传播最新版本 GravityRAT 的新 Android 恶意软件活动一直在进行，使用名为“BingeChat”的木马化聊天应用程序感染移动设备，该应用程序试图从受害者的设备中窃取数据。

参考链接：https://www.bleepingcomputer.com/news/security/android-gravityrat-malware-now-steals-your-whatsapp-backups/

2. 工作人员定期将敏感数据发布到 ChatGPT

一项新研究发现，15%的员工定期将公司数据发布到 ChatGPT 中，其中超过四分之一的数据被认为是敏感信息，这使他们的雇主面临安全漏洞的风险。

参考链接：https://cybernews.com/security/workers-regularly-post-sensitive-data-into-chatgpt/

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