国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 04 月 24 日-2023 年 05 月 07 日

2023 年第 17、18 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 324 个，其中高危漏洞 149 个、中危漏洞 155 个、低危漏洞 20 个。漏洞平均分值为 6.58。本周收录的漏洞中，涉及 0day 漏洞 214 个（占 66%），其中互联网上出现“Hospital Management Center 跨站请求伪造漏洞、SWFMill base64_encode 组件缓冲区溢出漏洞”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 12062 个，与上周（8401 个）环比增加 44%。

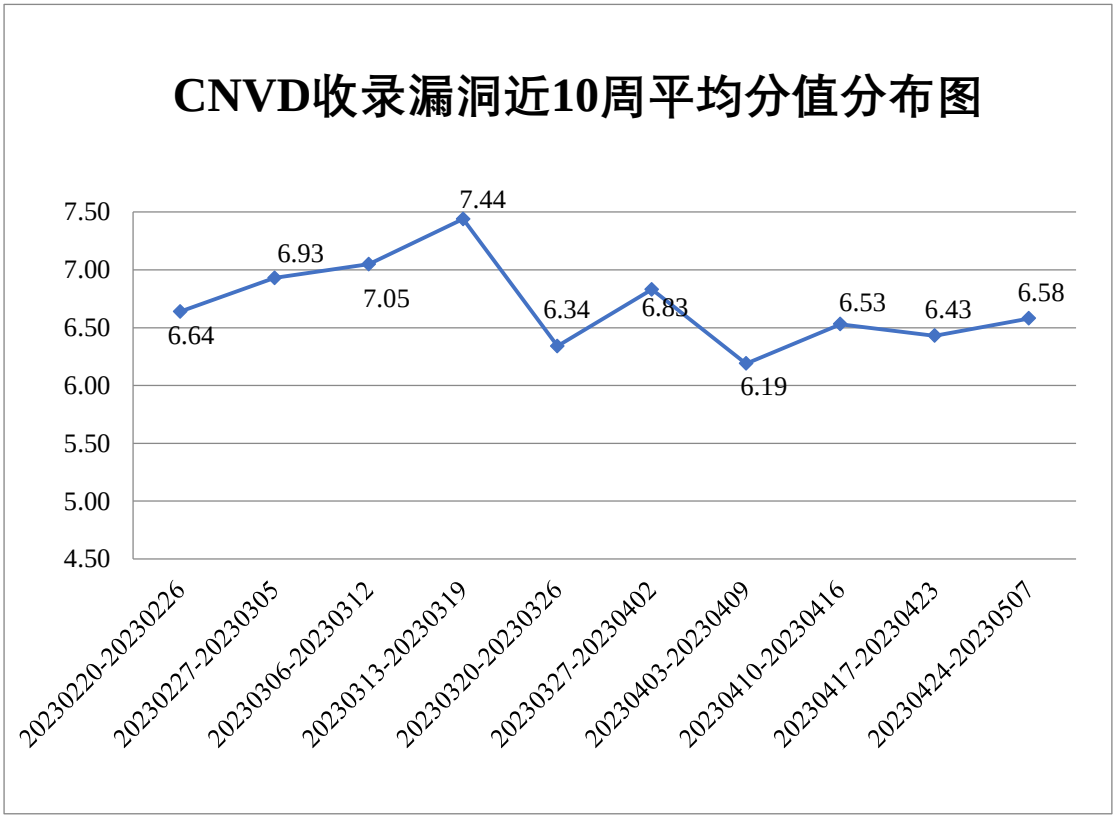

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 47 起，向基础电信企业通报漏洞事件 43 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 470 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 294 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 147 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：

珠海世安消防安全技术服务有限公司、重庆鱼木飞鸟科技有限公司、重庆梅安森科技股份有限公司、重庆建工信息技术有限公司、中远海运（广州）有限公司、郑州天迈科技股份有限公司、浙江中控技术股份有限公司、浙江网盛生意宝股份有限公司、浙江德塔森特数据技术有限公司、浙江大云物联科技有限公司、浙江大华技术股份有限公司、兆易创新科技集团股份有限公司、源澈科技开发（深圳）有限公司、渔翁信息技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、一键科技有限公司、星环信息科技（上海）股份有限公司、新开普电子股份有限公司、西安瑞友信息技术资讯有限公司、武汉易维科技股份有限公司、武汉大势智慧科技有限公司、伟乐视讯科技股份有限公司、薇拉文化集团有限公司、威博通科技（上海）有限公司、万兴科技集团股份有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天津神州浩天科技有限公司、泰尔茂医疗产品（上海）有限公司、苏州宏云智能科技有限公司、四平市九州易通科技有限公司、四川众望升腾科技有限公司、石家庄民友网络科技有限公司、沈阳点动科技有限公司、神州数码集团股份有限公司、深圳中赫斯曼科技有限公司、深圳维盟网络技术有限公司、深圳维盟科技股份有限公司、深圳市英威腾电气股份有限公司、深圳市易佰网络科技有限公司、深圳市伟图科技开发有限公司、深圳市普顺达科技有限公司、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、深圳市海柔创新科技有限公司、深圳市鼎游信息技术有限公司、深圳市博思高科技有限公司、深圳市必联电子有限公司、深圳凌特华盛科技有限公司、深圳警翼智能科技股份有限公司、深圳华磊物流通信息科技有限公司、深圳古瑞瓦特科技能源有限责任公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海韵达货运有限公司、上海远丰信息科技（集团）有限公司、上海英立视数字科技有限公司、上海商派网络科技有限公司、上海瑞美信息技术有限公司、上海锐昉科技有限公司、上海擎创信息技术有限公司、上海曼恒数字技术股份有限公司、上海麦沃丰行供应链科技有限公司、上海邻多多信息科技有限公司、上海快快查信息科技有限公司、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、上海汉得信息技术股份有限公司、上海泛微网络科技股份有限公司、上海东方龙新媒体有限公司、上海顶

想信息科技有限公司、上海伯俊软件科技有限公司、上海艾泰科技有限公司、山东中维世纪科技股份有限公司、山东影响力智能科技有限公司、山东义理信息技术有限公司、山东京帝软件有限公司、山东广安车联科技股份有限公司、山东点狮信息科技有限公司、厦门四信通信科技有限公司、厦门纳龙健康科技股份有限公司、瑞斯康达科技发展股份有限公司、青岛聚城网络科技有限公司、普联技术有限公司、鹏为软件股份有限公司、南京通达海科技股份有限公司、南京帆软软件有限公司、迈普通信技术股份有限公司、领航未来（北京）科技有限公司、立得空间信息技术股份有限公司、廊坊市极致网络科技有限公司、兰州中科维智信息咨询有限公司、金蝶软件（中国）有限公司、江苏麦维智能科技有限公司、江苏金智教育信息股份有限公司、济南驰骋信息技术有限公司、集力今越（天津）科技发展有限公司、吉翁电子（深圳）有限公司、华德智慧能源管理有限公司、湖南省众达数蔚信息技术有限公司、弘扬软件股份有限公司、弘成科技发展有限公司、河南新兵锋软件科技有限公司、河北先河环保科技股份有限公司、合肥岭雁科技有限公司、合肥贰道网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州新中大科技股份有限公司、杭州三汇信息工程有限公司、杭州海康威视数字技术股份有限公司、汉王科技股份有限公司、广州拙进通信技术有限公司、广州中望龙腾软件股份有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广州迪士普音响科技有限公司、广东新禾道信息科技有限公司、广东品胜电子股份有限公司、广东凯格科技有限公司、广东宏茂建设管理有限公司、广东飞企互联科技股份有限公司、福州联迅信息科技有限公司、福建远控科技有限公司、福建金网际软件科技有限公司、东北师大理想软件股份有限公司、成都生动网络科技有限公司、成都爱米秀科技有限责任公司、畅捷通信息技术股份有限公司、北京致远互联软件股份有限公司、北京指掌易科技有限公司、北京长久物流股份有限公司、北京赢科天地电子有限公司、北京易华录信息技术股份有限公司、北京亿赛通科技发展有限责任公司、北京亚控科技发展有限公司、北京旋极百旺科技有限公司、北京星网锐捷网络技术有限公司、北京星立方科技发展股份有限公司、北京五指互联科技有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京数码视讯科技股份有限公司、北京树袋熊网络科技有限公司、北京世纪超星信息技术发展有限责任公司、北京慕华信息科技有限公司、北京六方云信息技术有限公司、北京朗新天霁软件技术有限公司、北京久其软件股份有限公司、北京竞业达数码科技股份有限公司、北京建科研软件技术有限公司、北京惠朗时代科技有限公司、北京华驰联创科技有限公司、北京宏景世纪软件股份有限公司、北京国炬信息技术有限公司、北京飞书科技有限公司、北京对啊网教育科技有限公司、北京邦永科技有限公司、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、安科瑞电气股份有限公司、安徽卓智教育科技有限责任公司、安徽中技国医医疗科技有限公司、安徽省科大奥锐科技有限公司、阿里巴巴集团安全应急响应中心、emlog和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、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、深信服科技股份有限公司、阿里云计算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、贵州泰若数字科技有限公司、北京升鑫网络科技有限公司、上海齐同信息科技有限公司、河南信安世纪科技有限公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、山东正中信息技术股份有限公司、北京山石网科信息技术有限公司、联想集团、重庆电信系统集成公司、星云博创科技有限公司、湖南轻山信息技术有限公司、中孚安全技术有限公司、赛尔网络有限公司、中国银行、博智安全科技股份有限公司、深圳昂楷科技有限公司、中国联合网络通信有限公司福建省分公司、山东新潮信息技术有限公司、中国电信股份有限公司上海研究院、杭州美创科技有限公司、武汉提灯信息技术有限公司、郑州埃文科技、广西网信信息技术有限公司、超聚变数字技术有限公司、广州安亿信软件科技有限公司、合肥梆梆信息科技有限公司、河南灵创电子科技有限公司及其他个人白帽子向 CNVD 提交了 12062 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）、奇安信网神（补天平台）、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 8438 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）	2866	2866
斗象科技（漏洞盒子）	2565	2565
三六零数字安全科技集团有限公司	2096	2096
上海交大	911	911
新华三技术有限公司	581	0
北京神州绿盟科技有限公司	580	2
北京启明星辰信息安全技术有限公司	576	0
深信服科技股份有限公司	547	0
阿里云计算有限公司	405	8
安天科技集团股份有	325	0

限公司		
北京数字观星科技有限公司	181	0
北京天融信网络安全技术有限公司	134	6
远江盛邦（北京）网络安全科技股份有限公司	112	112
中国电信集团系统集成有限责任公司	75	2
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	30	30
京东科技信息技术有限公司	23	3
杭州迪普科技股份有限公司	16	2
北京知道创宇信息技术有限公司	5	0
浙江大华技术股份有限公司	1	1
北京信联数安科技有限公司	1	1
快页信息技术有限公司	808	808
贵州泰若数字科技有限公司	478	478
北京升鑫网络科技有限公司	90	90
上海齐同信息科技有限公司	40	40
河南信安世纪科技有限公司	24	24
安徽锋刃信息科技有	19	19

限公司		
河南东方云盾信息技术有限公司	18	18
山东正中信息技术股份有限公司	12	12
北京山石网科信息技术有限公司	9	9
联想集团	9	9
重庆电信系统集成公司	8	8
星云博创科技有限公司	7	7
湖南轻山信息技术有限公司	4	4
中孚安全技术有限公司	4	4
赛尔网络有限公司	2	2
中国银行	2	2
博智安全科技股份有限公司	2	2
深圳昂楷科技有限公司	2	2
中国联合网络通信有限公司福建省分公司	2	2
山东新潮信息技术有限公司	1	1
中国电信股份有限公司上海研究院	1	1
杭州美创科技有限公司	1	1
武汉提灯信息技术有限公司	1	1
郑州埃文科技	1	1
广西网信信息技术有限公司	1	1

超聚变数字技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
中国工商银行	1	1
合肥梆梆信息科技有限公司	1	1
河南灵创电子科技有限公司	1	1
CNCERT 北京分中心	2	2
CNCERT 山西分中心	1	1
个人	1903	1903
报送总计	15546	12062

本周漏洞按类型和厂商统计

本周，CNVD 收录了 324 个漏洞。WEB 应用 153 个，应用程序 112 个，网络设备（交换机、路由器等网络端设备）43 个，智能设备（物联网终端设备）8 个，安全产品 3 个，操作系统 3 个，数据库 2 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	153
应用程序	112
网络设备（交换机、路由器等网络端设备）	43
智能设备（物联网终端设备）	8
安全产品	3
操作系统	3
数据库	2

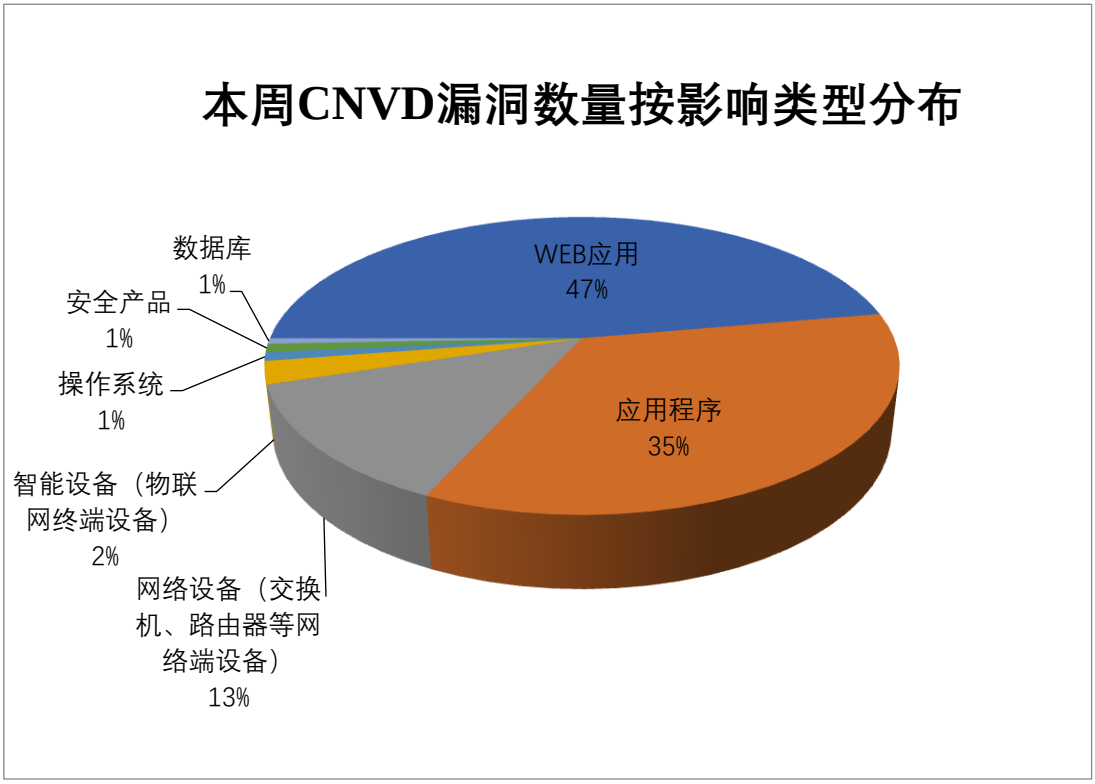

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Fortinet、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	Adobe	21	7%
2	Fortinet	14	4%
3	Apache	13	4%
4	深圳市吉祥腾达科技有限公司	11	3%
5	WordPress	10	3%
6	Microsoft	10	3%
7	Google	8	2%
8	Tenda	6	2%
9	Online Pizza Ordering System	5	2%
10	其他	226	70%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，20 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，“TOTOLINK X18 命令注入漏洞、Schneider Electric

PowerLogic 输入验证错误漏洞（CNVD-2023-34448）”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/

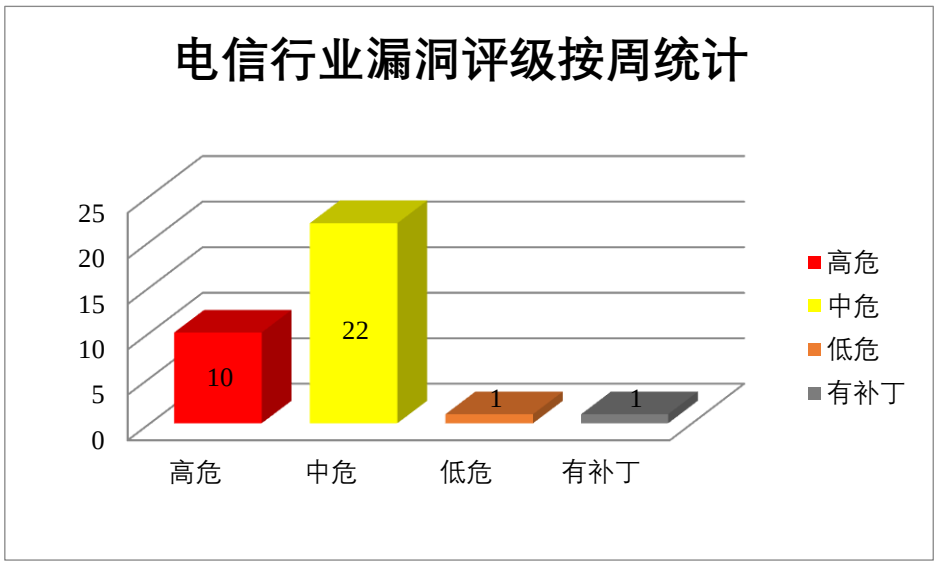

图 3 电信行业漏洞统计

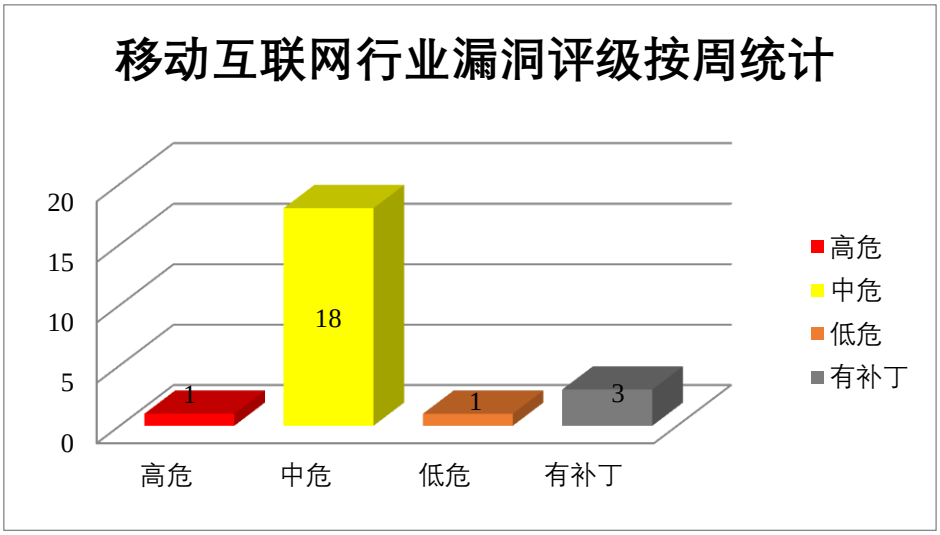

图 4 移动互联网行业漏洞统计

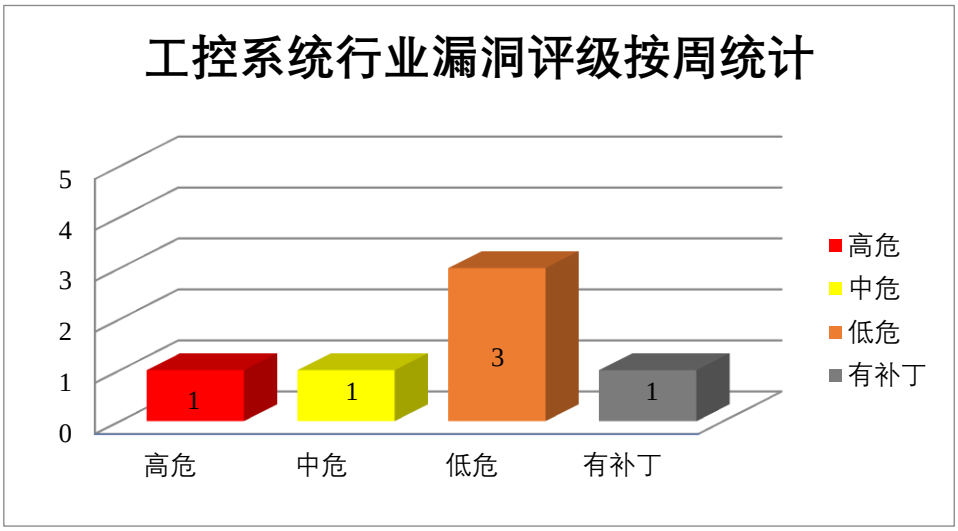

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft PostScript Printer Driver 是美国微软（Microsoft）公司的用于 PostScript 打印机的 Microsoft 标准打印机驱动程序。Microsoft PCL6 Class Printer Driver 是美国微软（Microsoft）公司的一个打印机驱动软件。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信息泄露，远程执行代码。

CNVD 收录的相关漏洞包括：Microsoft PostScript and PCL6 Class Printer Driver 信息泄露漏洞（CNVD-2023-30862、CNVD-2023-30865）、Microsoft PostScript and PCL6 Class Printer Driver 远程代码执行漏洞（CNVD-2023-30866、CNVD-2023-30864、CNVD-2023-30868、CNVD-2023-30867、CNVD-2023-30863、CNVD-2023-30861）。除“Microsoft PostScript and PCL6 Class Printer Driver 信息泄露漏洞（CNVD-2023-30862、CNVD-2023-30865）”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-2023-30863

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30862

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30861

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30866

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30865

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30864

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30868

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30867

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，攻击者可利用漏洞访问敏感信息，导致程序崩溃，任意代码执行等。

CNVD 收录的相关漏洞包括：Google Chrome ANGLE 组件内存错误引用漏洞、Google Chrome Extensions API 安全特征问题漏洞、Google Chrome PDF 安全特征问题漏洞、Google Chrome Messaging 组件内存错误引用漏洞、Google Chrome Performance Manager 组件内存错误引用漏洞、Google Chrome UI Foundations 组件内存错误引用漏洞、Google Chrome User Education 组件内存错误引用漏洞、Google Chrome 共享组件内存错误引用漏洞。除“Google Chrome PDF 安全特征问题漏洞”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-2023-33071

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33072

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33073

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33074

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33075

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33076

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33077

https://www.cnvd.org.cn/flaw/show/CNVD-2023-33078

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 Linkis 是美国阿帕奇（Apache）基金会的一个库。有助于轻松连接各种后端计算/存储引擎。Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache Log4j 是美国阿帕奇（Apache）基金会的一款基于 Java 的开源日志记录工具。Apache Solr 是一个开源的搜索服务，使用 Java 语言开发，主要基于 HTTP 和 Apache Lucene 实现的。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在反序列化对象时导致拒绝服务，在目标系统上执行任意代码。

CNVD 收录的相关漏洞包括：Apache Airflow 输入验证错误漏洞（CNVD-2023-30852、CNVD-2023-30851）、Apache Linkis 任意文件上传漏洞、Apache Linkis 目录遍历漏洞、Apache Linkis 反序列化漏洞、Apache HTTP Server Http 请求走私漏洞（CNVD-2023-30860）、Apache Log4j 资源管理错误漏洞、Apache Solr 命令执行漏洞。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-2023-30852

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30851

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30856

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30855

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30854

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30860

https://www.cnvd.org.cn/flaw/show/CNVD-2023-30858

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34111

4、Adobe 产品安全漏洞

Adobe Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行代码。

CNVD 收录的相关漏洞包括：Adobe Dimension 越界写入漏洞（CNVD-2023-31284、CNVD-2023-31286）、Adobe Dimension 越界读取漏洞（CNVD-2023-31287、CNVD-2023-31288、CNVD-2023-31290、CNVD-2023-31293、CNVD-2023-31292、CNVD-2023-31294）。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-2023-31284

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31286

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31287

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31288

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31290

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31293

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31292

https://www.cnvd.org.cn/flaw/show/CNVD-2023-31294

5、TP-LINK TL-WR940N 安全特征问题漏洞

TP-LINK TL-WR940N 是中国普联（TP-LINK）公司的一款无线路由器。本周，TP-LINK TL-WR940N 被披露存在安全特征问题漏洞，攻击者可利用该漏洞绕过系统上的身份验证。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-2023-32177

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-2023-30848	Fortinet FortiPresence 身份验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-22-355
CNVD-2023-30847	Fortinet FortiNAC 信息泄露漏洞）	高	目前官方已发布安全更新，建议用户尽快升级至最新版本：https://fortiguard.com/psirt/FG-IR-22-409
CNVD-2023-30845	Fortinet FortiClientWindows 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：https://fortiguard.com/psirt/FG-IR-22-429
CNVD-2023-30853	Apache Sling SlingRequestDispatcher 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/hhp611hltby3whk03vx2mv7cmy3vs0ok
CNVD-2023-30857	Apache Linkis 弱算法漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/3cr1cz3210wzwngldwrqzm43vwhghp0p
CNVD-2023-31158	Dell PowerProtect Data Manager 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000212242/dsa-2023-137-dell-powerprotect-data-manager-security-update-for-proprietary-code-vulnerability
CNVD-2023-31160	answer 访问控制错误漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://github.com/answerdev/answer/releases/tag/v1.0.7
CNVD-2023-32178	RIOT-OS 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：hhttps://github.com/RIOT-OS/RIOT/security/advisories/GHSA-fv97-2448-gcf6
CNVD-2023-32179	RIOT-OS 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://github.com/RIOT-OS/RIOT/security/advisories/GHSA-69h9-vj5r-xcg6
CNVD-2023	ForgeRock Access Managem	高	厂商已发布了漏洞修复程序，请及

-32184	ent 访问控制错误漏洞		时关注更新：https://backstage.forgerock.com/downloads/browse/am/all/productId:am

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞导致信息泄露，远程执行代码。此外，Google、Apache、Adobe 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，导致程序崩溃，任意代码执行。另外，TP-LINK TL-WR940N 被披露存在安全特征问题漏洞，攻击者可利用该漏洞绕过系统上的身份验证。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、Hospital Management Center 跨站请求伪造漏洞

验证描述

Hospital Management Center 是一种 web 系统，可以帮助管理与医疗保健相关的信息，并帮助医疗保健提供者有效地完成工作。

Hospital Management Center 存在跨站请求伪造漏洞，该漏洞源于文件 appointment.php 未充分验证请求是否来自可信用户。攻击者可利用漏洞伪造恶意请求诱骗受害者点击，执行敏感操作。

验证信息

POC 链接：https://github.com/golamsarwar08/hms/issues/2

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-32173

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. 新的 Android 恶意软件“FluHorse”以欺骗性策略瞄准东亚市场

东亚市场的各个行业都受到了新的电子邮件网络钓鱼活动的影响，该活动分发了一种以前未记录的 Android 恶意软件 FluHorse，该恶意软件滥用了 Flutter 软件开发框架。

参考链接：https://thehackernews.com/2023/05/new-android-malware-fluhorse-targeting.html

2. 流行的 WordPress 插件中的新漏洞使超过 2 万个网站暴露于网络攻击

此漏洞允许任何未经身份验证的用户窃取敏感信息，在这种情况下，通过诱骗特权用户访问精心制作的 URL 路径来提升 WordPress 网站上的特权。

参考链接：https://thehackernews.com/2023/05/new-vulnerability-in-popular-wordpress.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

邮箱：vreport@cert.org.cn

电话：010-82991537