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 17 日-2023 年 04 月 23 日　　2023 年第 16 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 595 个，其中高危漏洞 254 个、中危漏洞 309 个、低危漏洞 32 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 501 个（占 84%），其中互联网上出现“Tenda AC21 缓冲区溢出漏洞、D-Link DIR820LA1 命令注入漏洞”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 8401 个，与上周（9435 个）环比减少 11%。

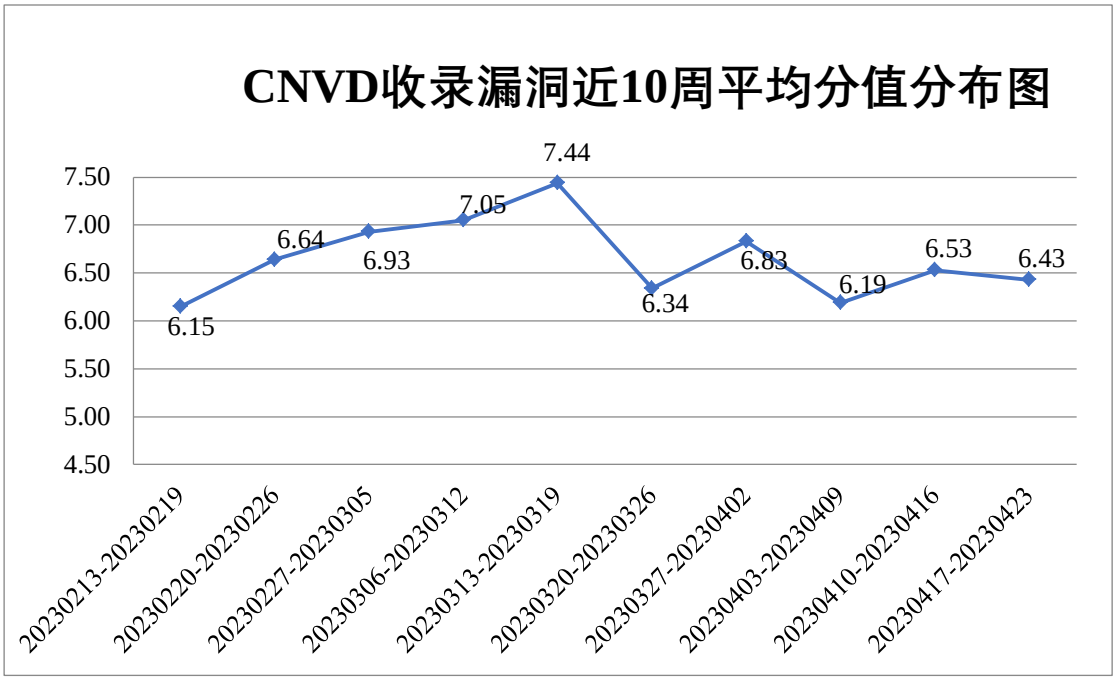

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 35 起，向基础电

信企业通报漏洞事件 40 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 2943 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 431 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 79 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：

珠海派诺科技股份有限公司、珠海必要科技有限公司、重庆亿数信息技术有限公司、重庆市小电天体新能源汽车有限公司、重庆美展科技有限公司、浙江中控技术股份有限公司、浙江兆龙互连科技股份有限公司、浙江宇视科技有限公司、浙江花田网络有限公司、浙江和达科技股份有限公司、浙江达华智慧安保集团有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、易家健康管理有限公司、新天科技股份有限公司、新开普电子股份有限公司、西安卓立科技实业有限公司、西安众邦网络科技有限公司、西安交大捷普网络科技有限公司、西安博冠教育科技有限公司、卫宁健康科技集团股份有限公司、万商云集（成都）科技股份有限公司、天维尔信息科技有限公司、天津天堰科技股份有限公司、腾讯安全应急响应中心、随商信息技术（上海）有限公司、随锐科技集团股份有限公司、宿迁鑫潮信息技术有限公司、苏州盛科通信股份有限公司、苏州科达科技股份有限公司、苏州浩辰软件股份有限公司、苏州国网电子科技有限公司、苏州德启智能科技有限公司、四川易泊时捷智能科技有限公司、世讯卫星技术有限公司、深圳维盟科技股份有限公司、深圳市微耕实业有限公司、深圳市同为数码科技股份有限公司、深圳市巨鼎医疗股份有限公司、深圳市吉祥腾达科技有限公司、深圳市丛文安全电子有限公司、绍兴市智辉信息科技有限公司、上海卓卓网络科技有限公司、上海旅烨网络科技有限公司、上海金电网安科技有限公司、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、上海泛微网络科技股份有限公司、上海东兰信息技术有限公司、上海德拓信息技术股份有限公司、上海布雷德科技有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山西企凝信息科技有限公司、厦门四信通信科技有限公司、厦门尚为科技股份有限公司、赛马物联科技（宁夏）有限公司、任子行网络技术股份有限公司、全讯汇聚网络科技（北京）有限公司、青岛易软天创网络科技有限公司、青岛聚城网络科技有限公司、普联技术有限公司、南京科远智慧科技集团股份有限公司、龙图腾网科技（合肥）股份有限公司、科来网络技术股份有限公司、江苏麦维智能科技有限公司、江苏弘电科技发展有限公司、济南卓源软件有限公司、吉翁电子（深圳）有限公司、基康仪器股份有限公司、河南科爵电子科技有限公司、和利时信安院、杭州云润科技有限公司、杭州雄伟科技开发股份有限公司、杭州飞致云信息科技有限公司、哈尔滨伟成科技有限公司、国资数据中心有限责任公司、广州中望龙腾软件股份有限公司、广州市和丰自动化科技有限公司、广东凯格科技有限公司、广东飞企互联科技股份有限公司、福州网钛软件科技有限公司、泛海物业管理有

限公司、帆软软件有限公司、东华医为科技有限公司、北京优锘科技有限公司、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、北京亚鸿世纪科技发展有限公司、北京小桔科技有限公司、北京神州数码云科信息技术有限公司、北京慕华信息科技有限公司、北京金和网络股份有限公司、北京和欣运达科技有限公司、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、北京奥博威斯科技有限公司、包头市助友科技有限公司、百洋智能科技集团股份有限公司、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、安徽商信政通信息技术股份有限公司和 semcms。

本周，CNVD 发布了《Oracle 发布 2023 年 4 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8781

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、深信服科技股份有限公司、北京神州绿盟科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京启明星辰信息安全技术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、博智安全科技股份有限公司、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、河南信安世纪科技有限公司、山东鼎夏智能科技有限公司、河南东方云盾信息技术有限公司、湖南轻山信息技术有限公司、安徽锋刃信息科技有限公司、杭州默安科技有限公司、联想集团、任子行网络技术股份有限公司、合肥梆梆信息科技有限公司、北京君云天下科技有限公司、江苏金盾检测技术股份有限公司、山东云天安全技术有限公司、广域铭岛数字科技有限公司、华鲁数智信息技术（北京）有限公司、中国电信股份有限公司上海研究院、河南灵创电子科技有限公司、星云博创科技有限公司、墨菲未来科技（北京）有限公司、深圳昂楷科技有限公司、江苏天竞云合数据技术有限公司、平安银河实验室、杭州美创科技有限公司、北京东方通科技股份有限公司、赛尔网络有限公司、国网十堰供电公司信息通信分公司、北京水木羽林科技有限公司、华泰证券股份有限公司、贵州华黔信安信息技术有限公司、汇安云（山东）信息科技有限公司、北京安帝科技有限公司、江苏晟晖信息科技有限公司及其他个人白帽子向 CNVD 提交了 8401 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 4943 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）	1967	1967
三六零数字安全科技	1576	1576

集团有限公司		
奇安信网神（补天平台）	1121	1121
新华三技术有限公司	667	0
深信服科技股份有限公司	564	6
北京神州绿盟科技有限公司	435	7
上海交大	279	279
远江盛邦（北京）网络安全科技股份有限公司	190	190
北京启明星辰信息安全技术有限公司	179	7
安天科技集团股份有限公司	178	0
北京天融信网络安全技术有限公司	165	3
天津市国瑞数码安全系统股份有限公司	42	0
杭州安恒信息技术股份有限公司	37	18
北京数字观星科技有限公司	30	0
京东科技信息技术有限公司	21	4
杭州迪普科技股份有限公司	14	0
北京知道创宇信息技术股份有限公司	4	0
西安四叶草信息技术有限公司	2	2
北京长亭科技有限公司	1	1
北京智游网安科技有	1	1

限公司		
恒安嘉新（北京）科技股份公司	1	0
快页信息技术有限公司	865	865
博智安全科技股份有限公司	69	69
北京升鑫网络科技有限公司	57	57
北京山石网科信息技术有限公司	44	44
河南信安世纪科技有限公司	27	27
山东鼎夏智能科技有限公司	26	26
河南东方云盾信息技术有限公司	25	25
湖南轻山信息技术有限公司	12	12
安徽锋刃信息科技有限公司	8	8
杭州默安科技有限公司	6	6
联想集团	3	3
亚信科技（成都）有限公司	2	0
任子行网络技术股份有限公司	2	2
合肥梆梆信息科技有限公司	2	2
北京君云天下科技有限公司	2	2
江苏金盾检测技术股份有限公司	2	2
山东云天安全技术有	2	2

限公司		
广域铭岛数字科技有限公司	2	2
华鲁数智信息技术（北京）有限公司	2	2
中国电信股份有限公司上海研究院	2	2
河南灵创电子科技有限公司	2	2
星云博创科技有限公司	2	2
墨菲未来科技（北京）有限公司	1	1
深圳昂楷科技有限公司	1	1
江苏天竞云合数据技术有限公司	1	1
平安银河实验室	1	1
杭州美创科技有限公司	1	1
北京东方通科技股份有限公司	1	1
赛尔网络有限公司	1	1
国网十堰供电公司信息通信分公司	1	1
北京水木羽林科技有限公司	1	1
华泰证券股份有限公司	1	1
贵州华黔信安信息技术有限公司	1	1
汇安云（山东）信息科技有限公司	1	1
北京安帝科技有限公司	1	1

江苏晟晖信息科技有限公司	1	1
CNCERT 甘肃分中心	4	4
CNCERT 贵州分中心	3	3
CNCERT 宁夏分中心	1	1
CNCERT 河北分中心	1	1
个人	2034	2034
报送总计	10695	8401

本周漏洞按类型和厂商统计

本周，CNVD 收录了 595 个漏洞。WEB 应用 333 个，应用程序 141 个，网络设备（交换机、路由器等网络端设备）88 个，智能设备（物联网终端设备）15 个，安全产品 12 个，操作系统 4 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	333
应用程序	141
网络设备（交换机、路由器等网络端设备）	88
智能设备（物联网终端设备）	15
安全产品	12
操作系统	4
数据库	2

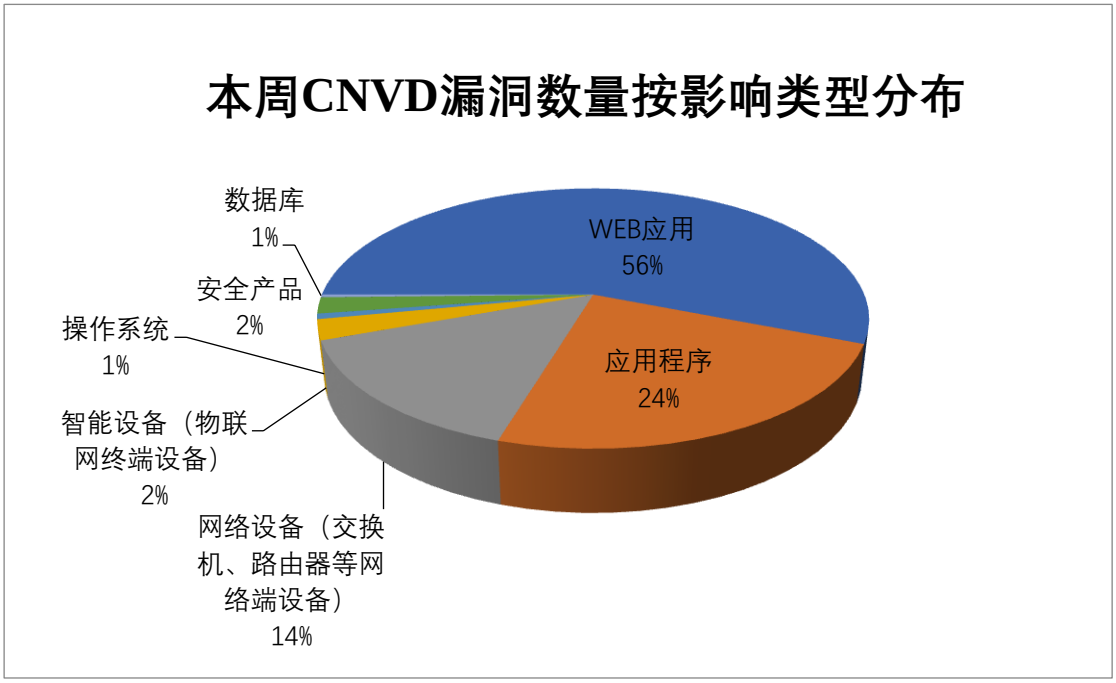

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、上海泛微网络科技股份有限公司、Carlo Montero 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	25	4%
2	上海泛微网络科技股份有限公司	17	3%
3	Carlo Montero	16	3%
4	北京百卓网络技术有限公司	15	3%
5	Microsoft	14	2%
6	北京神州数码云科信息技术有限公司	13	2%
7	H3C	12	2%
8	Cisco	11	2%
9	TOTOLINK	11	2%
10	其他	461	77%

本周行业漏洞收录情况

本周，CNVD 收录了 63 个电信行业漏洞，33 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2023-29379）、Siemens SICAM A8000 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/

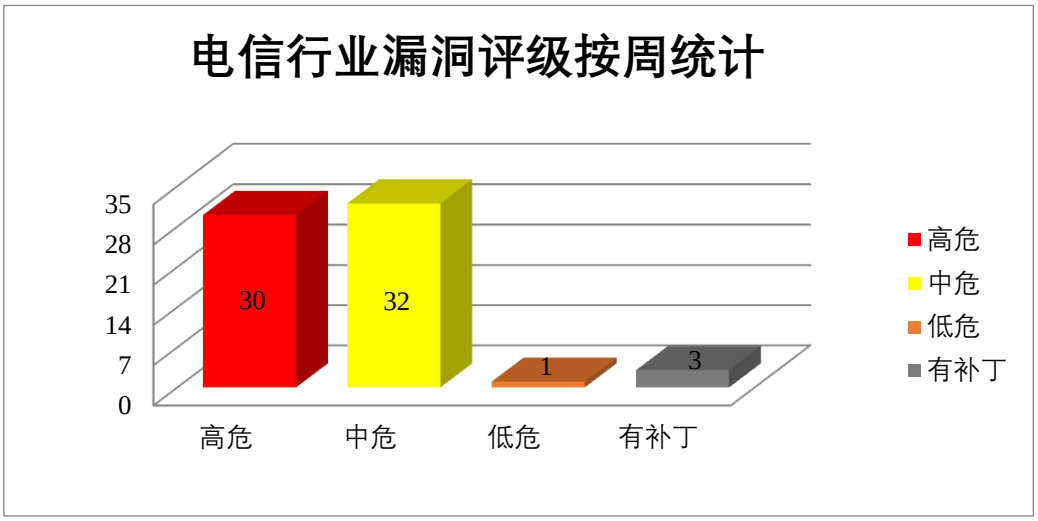

图 3 电信行业漏洞统计

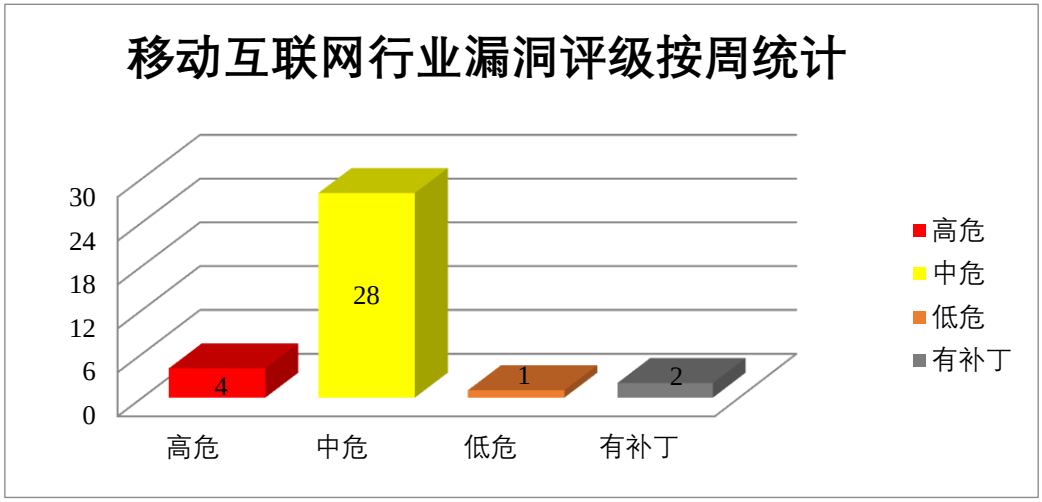

图 4 移动互联网行业漏洞统计

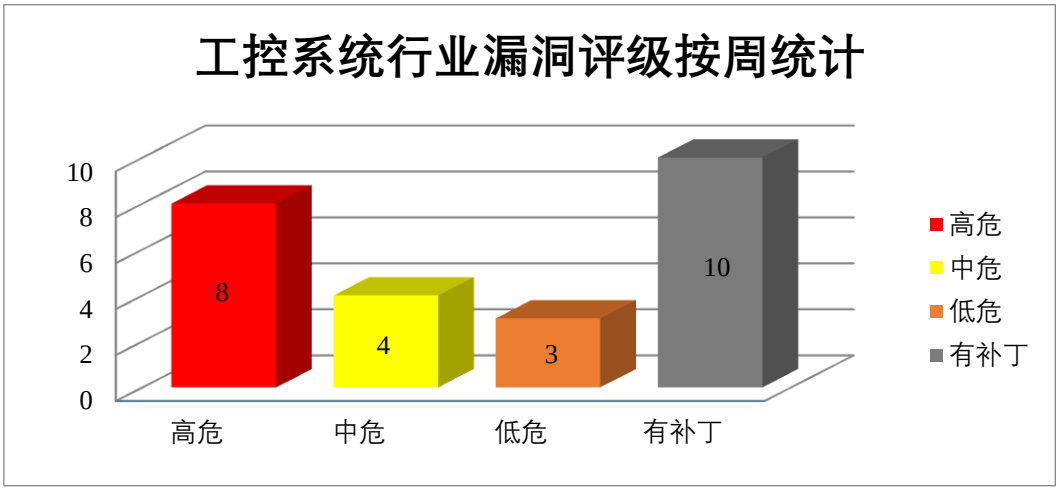

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Substance 3D Designer 是美国奥多比（Adobe）公司的一款 3D 设计软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Designer 堆缓冲区溢出漏洞（CNVD-2023-29793、CNVD-2023-29794）、Adobe Substance 3D Designer 堆栈缓冲区溢出漏洞、Adobe Substance 3D Designer 越界读取漏洞（CNVD-2023-29799、CNVD-2023-29801、CNVD-2023-29800）、Adobe Substance 3D Designer 内存错误引用漏洞（CNVD-2023-29802、CNVD-2023-29803）。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-2023-29794
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29793
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29797
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29799
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29801
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29800
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29803
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29802

2、SAP 产品安全漏洞

SAP Landscape Management 是德国思爱普（SAP）公司的一套 SAP 产品集中管理系统。SAP NetWeaver AS Java 是一款提供了 Java 运行环境的应用程序服务器。该产品主要用于开发和运行 Java EE 应用程序。SAP ABAP Platform 是一个基于 ABAP 的 SAP 解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取和修改一些敏感信息，提升权限等。

CNVD 收录的相关漏洞包括：SAP Landscape Management 信息泄露漏洞（CNVD-2023-28117）、SAP NetWeaver AS Java 访问控制错误漏洞、SAP ABAP Platform 路径遍历漏洞、SAP NetWeaver AS Java 授权问题漏洞（CNVD-2023-28121）、SAP NetWeaver AS 授权问题漏洞、SAP NetWeaver Application Server 访问控制错误漏洞、SAP NetWeaver 跨站脚本漏洞（CNVD-2023-28125）、SAP NetWeaver AS 输入验证错误漏洞（CNVD-2023-28124）。其中，“SAP Landscape Management 信息泄露漏洞（CNVD-2023-28117）、SAP ABAP Platform 路径遍历漏洞、SAP NetWeaver AS 授权问题漏洞”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-2023-28117
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28120
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28119
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28121
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28123
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28122
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28125
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28124

3、 Cisco 产品安全漏洞

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞对受影响设备进行存储型跨站脚本（XSS）攻击。

CNVD 收录的相关漏洞包括：Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2023-28093、CNVD-2023-28092、CNVD-2023-28096、CNVD-2023-28095、CNVD-2023-28094、CNVD-2023-28100、CNVD-2023-28099、CNVD-2023-28098）。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-2023-28093
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28092
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28096
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28095
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28094
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28100
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28099
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28098

4、 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 是一个打印机驱动软件。Microsoft Windows 是一款窗口化操作系统。Microsoft Azure 是一套开放的企业级云计算平台。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，特权提升，远程执行代码等。

CNVD 收录的相关漏洞包括：Microsoft PostScript and PCL6 Class Printer Driver 远程代码执行漏洞（CNVD-2023-28102、CNVD-2023-28103、CNVD-2023-28109、CNVD-2023-28111）、Microsoft PostScript and PCL6 Class Printer Driver 信息泄露漏洞（CNVD-2023-28105）、Microsoft PostScript and PCL6 Class Printer Driver 权限提升漏洞、

Microsoft Visual Studio 远程代码执行漏洞（CNVD-2023-29362）、Microsoft Azure Service Connector 安全功能绕过漏洞。其中，除“Microsoft PostScript and PCL6 Class Printer Driver 信息泄露漏洞（CNVD-2023-28105）”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-2023-28102
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28105
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28103
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28109
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28111
https://www.cnvd.org.cn/flaw/show/CNVD-2023-28110
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29362
https://www.cnvd.org.cn/flaw/show/CNVD-2023-29796

5、Dell PowerPath Management Appliance 信息泄露漏洞

Dell PowerPath Management Appliance 是美国戴尔（Dell）公司的一种 PowerPath 主机管理应用程序，提供两种模型：基于虚拟机的设备和 Docker 容器化设备。本周，Dell PowerPath Management Appliance 被披露存在信息泄露漏洞，攻击者可利用该漏洞查看储存在日志中的敏感信息。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-2023-29363

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-2023-28118	SAP NetWeaver 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://launchpad.support.sap.com/#/notes/3305369
CNVD-2023-28127	Google Chrome V8 类型混淆漏洞（CNVD-2023-28127）	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://chromereleases.googleblog.com/2023/04/stable-channel-update-for desktop_14.html
CNVD-2023-29372	Schneider Electric IGSS Data Server 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://igss.schneider-electric.com/
CNVD-2023	Schneider Electric IGSS Dat	高	厂商已发布了漏洞修复程序，请及

-29377	a Server 整数溢出漏洞		时关注更新：https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-102-01_IGSS_Security_Notification_V2.0.pdf
CNVD-2023-29380	Google Android 资源管理错误漏洞（CNVD-2023-29380）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.android.com/
CNVD-2023-29697	Wireshark LISP 解析器拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.wireshark.org/security/wnpa-sec-2023-10.html
CNVD-2023-29765	Strapi 服务器端模板注入（SSTI）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://strapi.io/
CNVD-2023-29790	answer 信息泄露漏洞（CNVD-2023-29790）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/answerdev/answer/releases/tag/v1.0.8
CNVD-2023-29804	Adobe Digital Editions 缓冲区溢出漏洞（CNVD-2023-29804）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/Digital-Editions/apsb23-04.html
CNVD-2023-29816	Huawei BiSheng-WNM FW 系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/en/psirt/security-advisories/2023/huawei-sa-scivi ahpp-4181d272-en

小结：本周，Adobe 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任意代码。此外，SAP、Cisco、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞对受影响设备进行存储型跨站脚本（XSS）攻击，导致信息泄露，特权提升，远程执行代码等。另外，Dell PowerPath Management Appliance 被披露存在信息泄露漏洞，攻击者可利用该漏洞查看储存在日志中的敏感信息。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、Tenda AC21 缓冲区溢出漏洞

验证描述

Tenda AC21 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC21 V16.03.08.15 版本存在缓冲区溢出漏洞，该漏洞源于/bin/httpd 的 form_fast_setting_wifi_set 函数对于输入数据缺少长度检查，攻击者可利用该漏洞通过有效载荷导致 httpd 重新启动。

验证信息

POC 链接：https://github.com/xxy1126/Vuln/tree/main/Tenda%20AC21/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-28112

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. 美国 CISA 最新收录三大漏洞，涉及谷歌和 ChatGPT

4 月 21 日，美国网络安全和基础设施安全局(CISA)在其漏洞(KEV)目录中新增三个安全漏洞，并建议美国联邦民事行政部门(FCEB)机构在 2023 年 5 月 12 日之前尽快修复这三个漏洞，以确保其网络安全。

参考链接：https://www.freebuf.com/news/364502.html

2. 阿里云 SQL 数据库曝两个漏洞，现已修复

阿里云 ApsaraDB RDS for PostgreSQL 和 AnalyticDB for PostgreQL 数据库爆出两个漏洞。潜在攻击者能够利用这两个漏洞破坏租户隔离保护，访问其它客户的敏感数据。

参考链接：https://thehackernews.com/2023/04/two-critical-flaws-found-in-alibaba.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