国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 08 月 22 日-2022 年 08 月 28 日 **2022 年第 34 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 179 个、中危漏洞 244 个、低危漏洞 52 个。漏洞平均分值为 6.17。本周收录的漏洞中，涉及 0day 漏洞 307 个（占 65%），其中互联网上出现“BaijiaCMS 任意文件上传漏洞、WUZHI CMS SQL 注入漏洞（CNVD-2022-59014）”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 5845 个，与上周（18020 个）环比减少 68%。

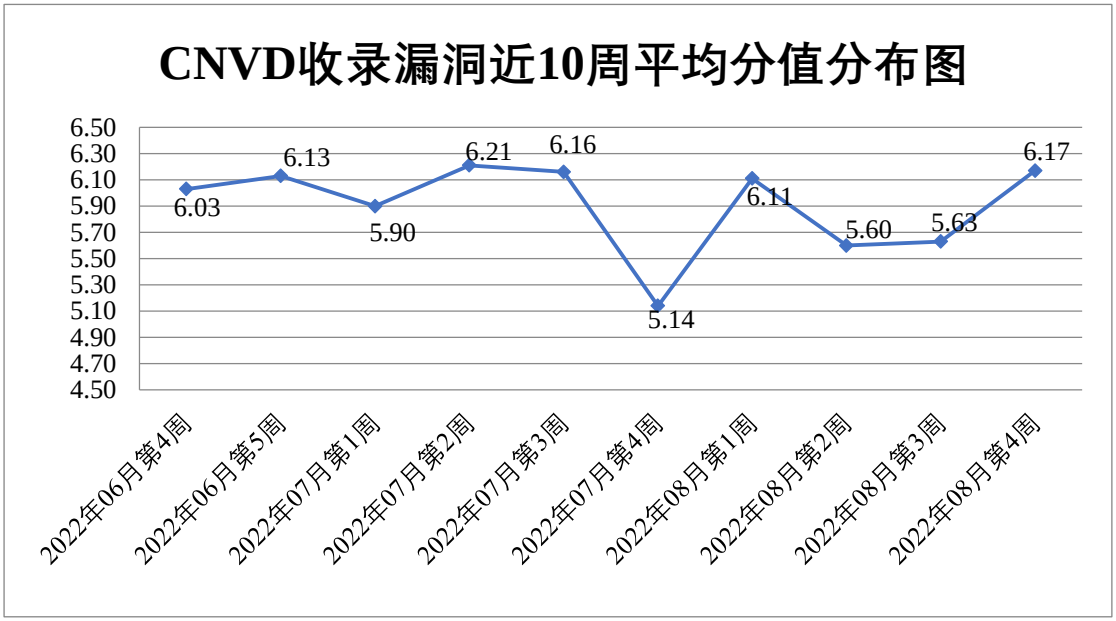

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 34 起，向基础电信企业通报漏洞事件 18 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 560 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 93 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 98 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：

紫光软件系统有限公司、淄博闪灵网络科技有限公司、镇江市云优网络科技有限公司、浙江心品网络科技有限公司、浙江大华技术股份有限公司、长沙市云研网络科技有限公司、漳州豆壳网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、译筑信息科技（上海）有限公司、烟台吉安电子科技有限公司、亚信科技（成都）有限公司、新疆恒和久远信息技术有限公司、小米科技有限责任公司、小船出海教育科技（北京）有限公司、夏普商贸（中国）有限公司、西安悟空检测科技有限公司、西安嘉客信息科技有限责任公司、武汉云贝网络科技有限公司、武汉天地伟业科技有限公司、武汉舜通智能科技有限公司、武汉捷讯信息技术有限公司、维沃移动通信有限公司、泰华智慧产业集团股份有限公司、宿州市涛盛网络科技有限公司、石家庄市快线软件科技有限公司、深圳云安宝科技有限公司、深圳英飞拓科技股份有限公司、深圳市卓讯信息技术有限公司、深圳市云帕斯科技开发有限公司、深圳市圆梦云科技有限公司、深圳市优驱电子有限公司、深圳市异度信息产业有限公司、深圳市乙辰科技股份有限公司、深圳市迅雷网文化有限公司、深圳市信锐网科技术有限公司、深圳市视高科技发展有限公司、深圳市美科星通信技术有限公司、深圳市领空技术有限公司、深圳市吉祥腾达科技有限公司、深圳市步科电气有限公司、深圳市必联电子有限公司、深圳创维数字技术有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海移品信息技术有限公司、上海欣诺通信技术股份有限公司、上海晓材科技有限公司、上海嵩恒网络科技股份有限公司、上海赛连信息科技有限公司、上海青枣网络科技有限公司、上海蓝山办公软件有限公司、上海快猫文化传媒有限公司、上海景格科技股份有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海百胜软件股份有限公司、上海爱数信息技术股份有限公司、山西点可云科技有限公司、山石网科通信技术（北京）有限公司、山东运筹软件有限公司、山东康程信息科技有限公司、山东金钟科技集团股份有限公司、山东国子软件股份有限公司、山东德尔智能数码股份有限公司、厦门得推网络科技有限公司、日照钢铁控股集团有限公司、任子行网络技术股份有限公司、奇安信科技集团股份有限公司、普元信息技术股份有限公司、普联技术有限公司、纽仁信息科技（上海）有限公司、南京数旗科技有限公司、茉柏枘（上海）软件科技有限公司、摩莎科技（上海）有限公司、迈普通信技术股份有限公司、洛阳恒越计算机技术有限公司、理光(中国)投资有限公司、乐金电子（中国）有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、金华市宁志网络科技有限公司、江下信息科技（惠州）有限公司、江西铭软科技有限公司、江苏金智

教育信息股份有限公司、济南六脉信息科技有限公司、吉翁电子（深圳）有限公司、淮南市讯网信息技术有限公司、湖南建研信息技术股份有限公司、恒锋信息科技股份有限公司、河南吉海网络科技有限公司、合肥彼岸互联信息技术有限公司、杭州图南电子股份有限公司、杭州联汇科技股份有限公司、杭州迪普科技股份有限公司、杭州博采网络科技股份有限公司、杭州北控科技有限公司、海南赞赞网络科技有限公司、贵州觅新科技有限公司、广州齐博网络科技有限公司、广州红帆科技有限公司、阜阳心品云数字科技有限公司、佛山市杜特软件科技有限公司、大庆紫金桥软件技术有限公司、成都生动网络科技有限公司、畅捷通信息技术股份有限公司、北京紫荆视通科技有限公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京智慧远景科技产业股份有限公司、北京致远互联软件股份有限公司、北京映翰通网络技术股份有限公司、北京行控科技有限公司、北京星网锐捷网络技术有限公司、北京微力数字科技有限公司、北京通达信科科技有限公司、北京金万维科技有限公司、北京华宇信息技术有限公司、北京华耀科技有限公司、北京华夏春松科技有限公司、北京国炬信息技术有限公司、北京步鼎方舟科技有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安徽协达软件科技有限公司、安徽微同科技有限公司、欧迅斯设计 、蓝宝石留言本、京瓷集团、若依和悟空 CRM。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京数字观星科技有限公司、深信服科技股份有限公司、新华三技术有限公司、安天科技集团股份有限公司、杭州安恒信息技术股份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、贵州泰若数字科技有限公司、中国电信股份有限公司网络安全产品运营中心、河南东方云盾信息技术有限公司、杭州迪普科技股份有限公司、北京珞安科技有限责任公司、河南信安世纪科技有限公司、河南灵创电子科技有限公司、山石网科通信技术股份有限公司、苏州棱镜七彩信息科技有限公司、西藏熙安信息技术有限责任公司、浙江乾冠信息安全研究院、杭州海康威视数字技术股份有限公司、浙江木链物联网科技有限公司、重庆都会信息科技有限公司、中科汇能科技有限公司、天津安评信息技术有限公司、上海纽盾科技股份有限公司、天津龙翰科技有限公司、上海安势信息技术有限公司、重庆信息通信研究院、中能融合智慧科技有限公司攻防实验室、工业和信息化部电子第五研究所、广州安亿信软件科技有限公司、北京安帝科技有限公司、陕西青山四纪信息技术有限公司、北京升鑫网络科技有限公司、博智安全科技股份有限公司及其他个人白帽子向 CNVD 提交了 5845 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）、三六零数字安全科技集团有限公司、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 3981 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）	2103	2103
斗象科技（漏洞盒子）	1443	1443
北京数字观星科技有限公司	378	0
上海交大	347	347
深信服科技股份有限公司	308	3
新华三技术有限公司	255	0
安天科技集团股份有限公司	239	0
杭州安恒信息技术股份有限公司	131	113
北京天融信网络安全技术有限公司	105	2
恒安嘉新（北京）科技股份公司	101	1
三六零数字安全科技集团有限公司	88	88
南京众智维信息科技有限公司	87	87
北京启明星辰信息安全技术有限公司	77	21
中国电信集团系统集成有限责任公司	66	37
天津市国瑞数码安全系统股份有限公司	59	0
西安四叶草信息技术有限公司	48	48
京东科技信息技术有限公司	18	18
北京知道创宇信息技术有限公司	18	1

内蒙古云科数据服务股份有限公司	13	13
北京神州绿盟科技有限公司	3	3
南京联成科技发展股份有限公司	3	3
北京长亭科技有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	2	2
北京智游网安科技有限公司	1	1
北京华顺信安信息技术有限公司	267	2
贵州泰若数字科技有限公司	214	214
中国电信股份有限公司网络安全产品运营中心	47	47
河南东方云盾信息技术有限公司	30	30
杭州迪普科技股份有限公司	21	7
北京珞安科技有限责任公司	20	20
河南信安世纪科技有限公司	19	19
河南灵创电子科技有限公司	10	10
山石网科通信技术股份有限公司	5	5
苏州棱镜七彩信息科技有限公司	4	4
西藏熙安信息技术有	3	3

限责任公司		
浙江乾冠信息安全研究院	3	3
杭州海康威视数字技术股份有限公司	2	2
浙江木链物联网科技有限公司	2	2
重庆都会信息科技有限公司	2	2
中科汇能科技有限公司	2	2
天津安评信息技术有限公司	2	2
上海纽盾科技股份有限公司	2	2
天津龙翰科技有限公司	2	2
上海安势信息技术有限公司	2	2
亚信科技（成都）有限公司	1	0
重庆信息通信研究院	1	1
中能融合智慧科技有限公司攻防实验室	1	1
工业和信息化部电子第五研究所	1	1
广州安亿信软件科技有限公司	1	1
北京安帝科技有限公司	1	1
陕西青山四纪信息技术有限公司	1	1
北京升鑫网络科技有限公司	1	1
博智安全科技股份有	1	1

限公司		
CNCERT 贵州分中心	4	4
CNCERT 宁夏分中心	2	2
个人	1114	1114
报送总计	7684	5845

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 208 个，应用程序 138 个，网络设备（交换机、路由器等网络端设备）96 个，安全产品 21 个，智能设备（物联网终端设备）12 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	208
应用程序	138
网络设备（交换机、路由器等网络端设备）	96
安全产品	21
智能设备（物联网终端设备）	12

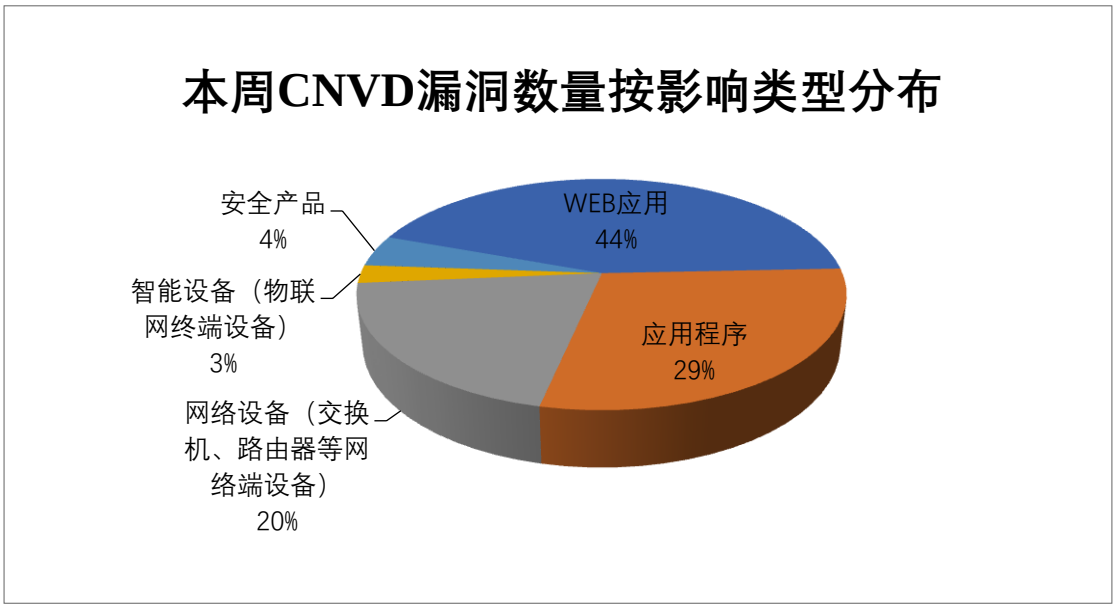

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、WordPress、InHand Networks 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	Microsoft	32	7%
2	WordPress	28	6%
3	InHand Networks	19	4%
4	Adobe	14	3%
5	Online Sports Complex Booking System	14	3%
6	SAP	12	2%
7	Fortinet	12	2%
8	D-Link	10	2%
9	中兴通讯股份有限公司	10	2%
10	其他	324	69%

本周行业漏洞收录情况

本周，CNVD 收录了 71 个电信行业漏洞，22 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，“InHand Networks InRouter302 命令执行漏洞、InHand Networks InRouter302 操作系统命令注入漏洞”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/

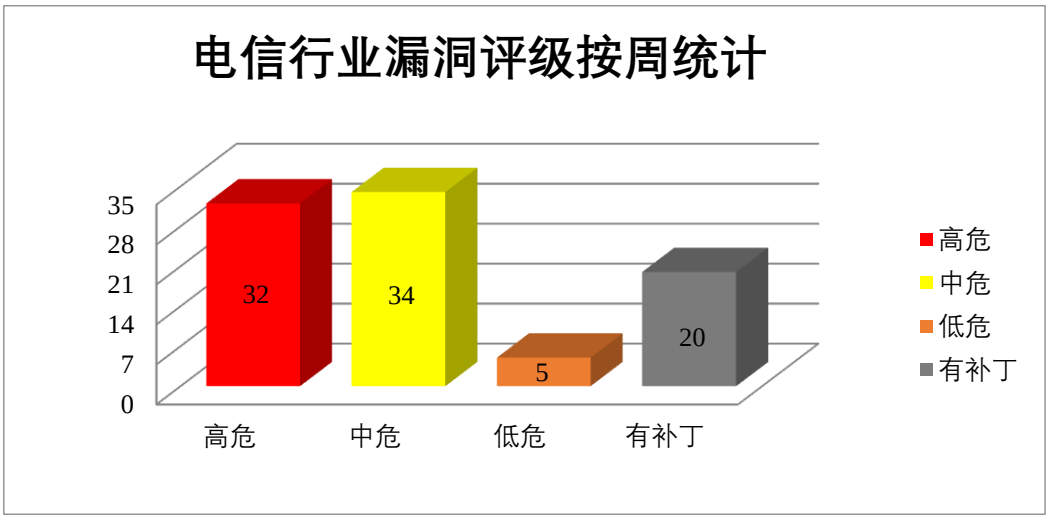

图 3 电信行业漏洞统计

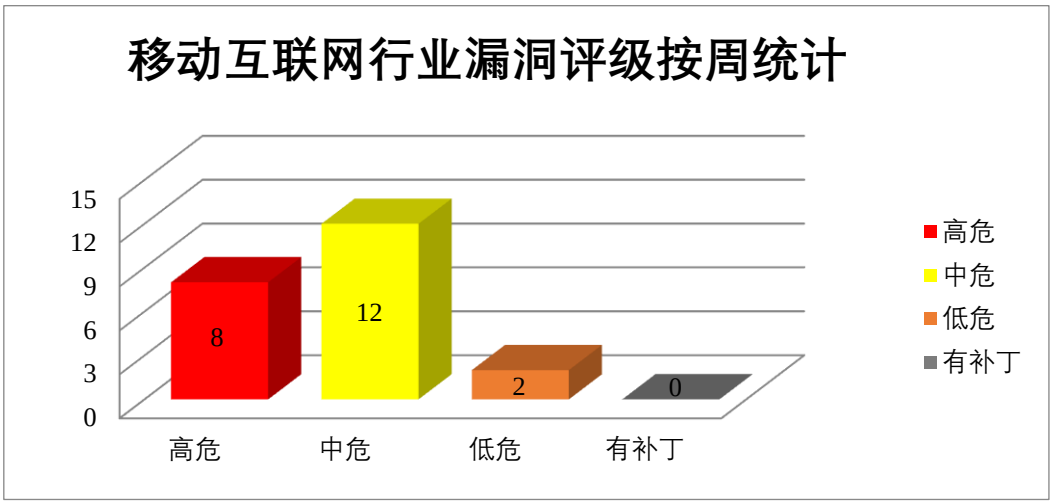

图 4 移动互联网行业漏洞统计

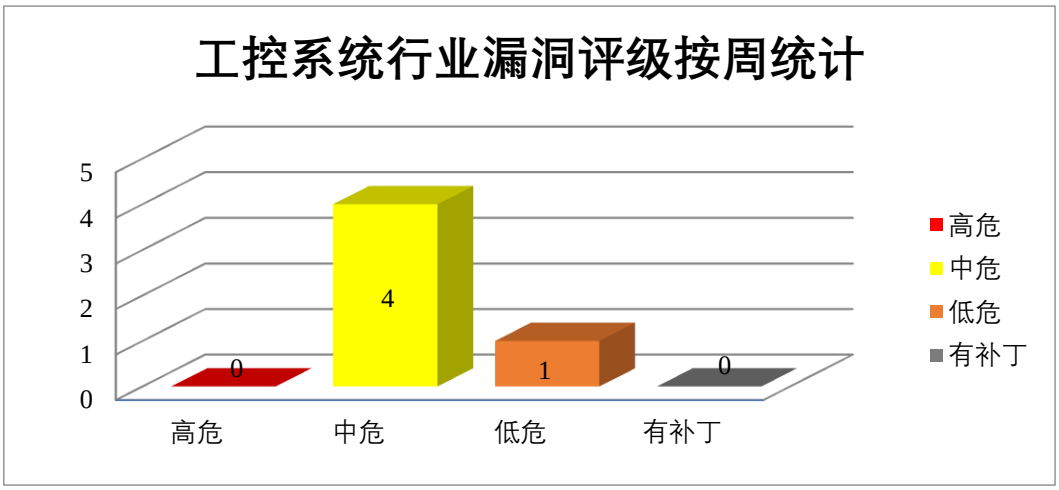

图 5 工控系统行业漏洞统计

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、 Fortinet 产品安全漏洞

Fortinet FortiSandbox 是美国飞塔（Fortinet）公司的一款 APT（高级持续性威胁）防护设备。该设备提供双重沙盒技术、动态威胁智能系统、实时控制面板和报告等功能。Fortinet FortiManager 是一套集中化网络安全管理平台。该平台支持集中管理任意数量的 Fortinet 设备，并能够将设备分组到不同的管理域（ADOM）进一步简化多设备安全部署与管理。Fortinet FortiAnalyzer 是一套集中式网络安全报告解决方案。该产品主要用于收集网络日志数据，并通过报告套件对日志中的安全事件、网络流量、Web 内容等进行分析、报告、归档操作。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向应用程序发送特别设计的请求，并在目标系统上执行任意代码，执行非法 SQL 语句，使设备进入无响应状态等。

CNVD 收录的相关漏洞包括：Fortinet FortiManager 访问控制错误漏洞（CNVD-20

22-58487）、Fortinet FortiManager 和 Fortinet FortiAnalyzer 环境问题漏洞、Fortinet FortiManager 和 Fortinet FortiAnalyzer 服务器端请求伪造漏洞、Fortinet FortiSandbox 缓冲区溢出漏洞、Fortinet FortiSandbox SQL 注入漏洞、Fortinet FortiSandbox 和 Fortinet FortiAuthenticator 拒绝服务漏洞、Fortinet FortiSandbox 操作系统命令注入漏洞、Fortinet FortiSandbox 跨站脚本漏洞。其中，“Fortinet FortiSandbox 和 Fortinet FortiAuthenticator 拒绝服务漏洞”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-2022-58487
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58486
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58485
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58489
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58488
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58492
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58491
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58490

2、SAP 产品安全漏洞

SAP Business One 是德国思爱普（SAP）公司的一套企业管理软件。该软件包括财务管理、运营管理和人力资源管理等功能。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认证过程，访问敏感信息，执行任意命令等。

CNVD 收录的相关漏洞包括：SAP Business One CSV 注入漏洞、SAP Business One 信息泄露漏洞（CNVD-2022-58472）、SAP Business One SQL 注入漏洞、SAP Business One 路径遍历漏洞、SAP Business One 输入验证错误漏洞、SAP Business One 权限许可和访问控制问题漏洞、SAP Business One 授权问题漏洞、SAP Business One 代码问题漏洞。其中，“SAP Business One 权限许可和访问控制问题漏洞、SAP Business One CSV 注入漏洞”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-2022-58470
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58472
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58471
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58474
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58473
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58478
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58477
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58476

3、Adobe 产品安全漏洞

Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Framemaker 是一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Illustrator 是一套基于向量的图像制作软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致内存泄漏等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2022-58460）、Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2022-58464、CNVD-2022-58463）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2022-58462、CNVD-2022-58461）、Adobe FrameMaker 缓冲区溢出漏洞（CNVD-2022-58467、CNVD-2022-58468）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2022-58466）。其中，除“Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2022-58463）、Adobe Acrobat Reader 输入验证错误漏洞”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-2022-58460
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58464
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58463
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58462
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58461
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58467
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58466
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58468

4、Microsoft 产品安全漏洞

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。Microsoft HEVC Video Extensions 是一个视频扩展应用程序。该应用使计算机和设备可以读取高效视频编码或 HEVC 视频。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。

CNVD 收录的相关漏洞包括：Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2022-59594）、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2022-59677、CNVD-2022-59676、CNVD-2022-59681、CNVD-2022-59680、CNVD-2022-59679、CNVD-2022-59684、CNVD-2022-59686）。其中，“Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2022-59594）、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2022-59686）”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-2022-59594

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59677

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59676

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59681

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59680

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59679

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59684

https://www.cnvd.org.cn/flaw/show/CNVD-2022-59686

5、D-Link DIR-816 缓冲区溢出漏洞

D-Link DIR-816 是中国台湾友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-816 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞导致栈溢出进而执行代码。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-2022-59201

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.htm

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-2022-58681	Open Automation Software OAS Platform 文件写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://openautomationsoftware.com/knowledge-base/getting-started-with-oas/
CNVD-2022-58679	Open Automation Software OAS Platform 访问控制错误漏洞（CNVD-2022-58679）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://openautomationsoftware.com/knowledge-base/getting-started-with-oas/
CNVD-2022-59058	Mapbox 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：https://github.com/mapbox/mapbox-maps-android/releases/tag/android-v10.6.1
CNVD-2022-59057	Apache Airflow 远程代码执行漏洞（CNVD-2022-59057）	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/614p38nf4gbk8xhvnskj9b1sqo2dknkb
CNVD-2022-59056	IBM Security Verify Governance 访问权限漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新:https://www.ibm.com/support/pages/node/6612733

CNVD-2022-59194	Lenovo Personal Cloud Storage 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://iknow.lenovo.com.cn/detail/dc_200017.html
CNVD-2022-59203	Vim 资源管理错误漏洞（CNVD-2022-59203）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim
CNVD-2022-59318	Huawei CV81-WDM FW 输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20220620-01-6e028b61-cn
CNVD-2022-59817	WordPress Photo Gallery plugin SQL 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://wpscan.com/vulnerability/2b4866f2-f511-41c6-8135-cf1e0263d8de
CNVD-2022-59848	Billing System 存在任意代码执行漏洞	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.sourcecodester.com/php/14831/billing-system-roject-php-source-code-free-download.html

小结：本周，Fortinet 产品被披露存在多个漏洞，攻击者可利用漏洞向应用程序发送特别设计的请求，并在目标系统上执行任意代码，执行非法 SQL 语句，使设备进入无响应状态等。此外，SAP、Adobe、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过认证过程，访问敏感信息，执行任意命令，导致内存泄漏等。另外，D-Link DIR-816 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞导致栈溢出进而执行代码。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、WUZHI CMS SQL 注入漏洞（CNVD-2022-59014）

验证描述

WUZHI CMS 是五指（WUZHI）公司的一套基于 PHP 和 MySQL 的开源内容管理系（CMS）。

WUZHI CMS v4.1.0 版本存在 SQL 注入漏洞，攻击者可利用该漏洞通过/coreframe/app/pay/admin/index.php 中的$keyValue 参数执行任意 SQL 命令。

验证信息

POC 链接：https://github.com/wuzhicms/wuzhicms/issues/198

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-59014

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. Atlassian Bitbucket 服务器和数据中心出现漏洞

该漏洞可能允许攻击者执行恶意代码，Atlassian 目前已经推出了漏洞修复方案。

参考链接：https://www.freebuf.com/news/343151.html

2. GitLab 修复了 CE、EE 版本中一个远程代码执行漏洞

DevOps 平台 GitLab 修复了其社区版（CE）和企业版（EE）中出现的一个远程代码执行漏洞。

参考链接：https://www.freebuf.com/news/342725.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