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 29 日-2022 年 09 月 04 日 **2022 年第 35 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 456 个，其中高危漏洞 155 个、中危漏洞 261 个、低危漏洞 40 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 331 个（占 73%），其中互联网上出现“Library Management System SQL 注入漏洞（CNVD-2022-61297）、Advanced School Management System SQL 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 8944 个，与上周（5845 个）环比增加 35%。

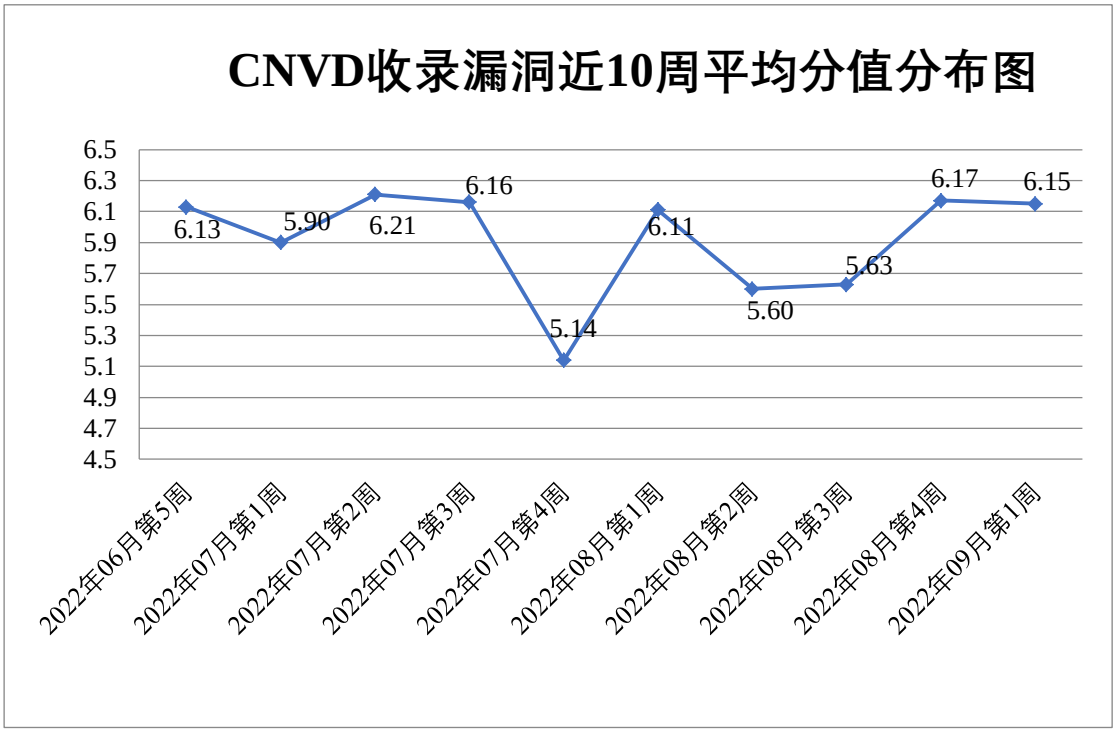

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 33 起，向基础电信企业通报漏洞事件 16 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 645 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 125 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 86 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：

淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、珠海高凌信息科技股份有限公司、中科博华信息科技有限公司、浙江中控技术股份有限公司、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、研华科技（中国）有限公司、武汉达梦数据库股份有限公司、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、天津神州浩天科技有限公司、唐山市柳林自动化设备有限公司、四创科技有限公司、石家庄市快线软件科技有限公司、沈阳明致软件有限公司、深圳市子辰视讯科技有限公司、深圳市铭数信息有限公司、深圳市蓝凌软件股份有限公司、深圳市科图自动化新技术有限公司、深圳市吉祥腾达科技有限公司、深圳市共济科技股份有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海宜会信息技术有限公司、上海市企炬企业发展有限公司、上海上业信息科技股份有限公司、上海普加软件有限公司、上海普华科技发展股份有限公司、上海穆云智能科技有限公司、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、上海博睿泰和软件技术有限公司、上海贝锐信息科技股份有限公司、山东企云软件有限公司、山东博硕自动化技术有限公司、睿易教育科技股份有限公司、锐捷网络股份有限公司、普联技术有限公司、南京云网汇联软件技术有限公司、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、零视技术(上海)有限公司、联想（北京）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、葵花科技信息网、江西怡杉环保股份有限公司、江西铭软科技有限公司、江苏省广电有线信息网络股份有限公司、江苏金智科技股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南建研信息技术股份有限公司、黑龙江立高科技股份有限公司、河南幻神网络科技有限公司、河北赫烁科技有限公司、杭州海康威视数字技术股份有限公司、杭州北控科技有限公司、汉王科技股份有限公司、海南赞赞网络科技有限公司、国交信息股份有限公司、广州酷狗计算机科技有限公司、广州红迅软件有限公司、广州红帆科技有限公司、广东大普通信技术股份有限公司、福建金网际软件科技有限公司、福建博思软件股份有限公司、成都飞鱼星科技股份有限公司、畅捷通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、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京搜狐新媒体信息技术有限公司、北京世纪超星信息技术发展有限责任公司、北京墨迹风云科技股份有限公司、北京龙软科技股份

有限公司、北京蓝湾博阅科技有限公司、北京久幺幺科技有限公司、北京华宇信息技术有限公司、北京华耀科技有限公司、北京高速波软件有限公司、北京北大方正电子有限公司、北京百度网讯科技有限公司、北京安天网络安全技术有限公司、阿里巴巴集团安全应急响应中心、POLYCOM 通讯技术（北京）有限公司、中祭网信息科技、中国网站服务网上海总部和 JFinalOA。

本周，CNVD 发布了《关于畅捷通 T+软件存在任意文件上传漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8056

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、新华三技术有限公司、阿里云计算有限公司、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、河南东方云盾信息技术有限公司、河南信安世纪科技有限公司、山东新潮信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、山石网科通信技术股份有限公司、福建省海峡信息技术有限公司、浙江木链物联网科技有限公司、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、苏州棱镜七彩信息科技有限公司、北京君云天下科技有限公司、长春嘉诚信息技术股份有限公司、上海纽盾科技股份有限公司、中国电信股份有限公司上海研究院、河南天祺信息安全技术有限公司、上海上讯信息技术股份有限公司、统信软件技术有限公司、江苏省信息安全测评中心、上海安势信息技术有限公司、北京众安天下科技有限公司、北京远禾科技有限公司、云南联创网安科技有限公司、广州安亿信软件科技有限公司、畅捷通信息技术股份有限公司、北京珞安科技有限责任公司及其他个人白帽子向 CNVD 提交了 8944 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 7209 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）	4801	4801
三六零数字安全科技集团有限公司	1035	1035
奇安信网神（补天平台）	843	843
北京神州绿盟科技有限公司	626	0

上海交大	530	530
新华三技术有限公司	371	0
阿里云计算有限公司	369	0
深信服科技股份有限公司	321	0
安天科技集团股份有限公司	237	3
北京数字观星科技有限公司	205	0
北京天融信网络安全技术有限公司	177	5
南京众智维信息科技有限公司	149	149
远江盛邦（北京）网络安全科技股份有限公司	88	88
恒安嘉新（北京）科技股份公司	79	0
北京启明星辰信息安全技术有限公司	61	6
天津市国瑞数码安全系统股份有限公司	59	0
中国电信集团系统集成有限责任公司	27	0
杭州安恒信息技术股份有限公司	20	20
西安四叶草信息技术有限公司	12	12
内蒙古云科数据服务股份有限公司	11	11
北京知道创宇信息技术有限公司	13	1
南京联成科技发展股份有限公司	4	4

京东科技信息技术有限公司	3	3
内蒙古奥创科技有限公司	3	3
北京信联科汇科技有限公司	3	3
北京华顺信安信息技术有限公司	207	3
河南东方云盾信息技术有限公司	48	48
河南信安世纪科技有限公司	29	29
山东新潮信息技术有限公司	16	16
奇安星城网络安全运营服务（长沙）有限公司	11	11
山石网科通信技术股份有限公司	7	7
杭州迪普科技股份有限公司	6	0
福建省海峡信息技术有限公司	4	4
浙江木链物联网科技有限公司	4	4
快页信息技术有限公司	4	4
博智安全科技股份有限公司	4	4
北京升鑫网络科技有限公司	3	3
苏州棱镜七彩信息科技有限公司	3	3
北京君云天下科技有	3	3

限公司		
长春嘉诚信息技术股份有限公司	2	2
上海纽盾科技股份有限公司	2	2
中国电信股份有限公司上海研究院	2	2
河南天祺信息安全技术有限公司	1	1
上海上讯信息技术股份有限公司	1	1
统信软件技术有限公司	1	1
江苏省信息安全测评中心	1	1
上海安势信息技术有限公司	1	1
北京众安天下科技有限公司	1	1
北京远禾科技有限公司	1	1
云南联创网安科技有限公司	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
畅捷通信息技术股份有限公司	1	1
北京珞安科技有限责任公司	1	1
亚信科技（成都）有限公司	1	0
CNCERT 浙江分中心	9	9
CNCERT 贵州分中心	3	3

CNCERT 四川分中心	1	1
个人	1257	1257
报送总计	11685	8944

本周漏洞按类型和厂商统计

本周，CNVD 收录了 456 个漏洞。WEB 应用 228 个，应用程序 126 个，网络设备（交换机、路由器等网络端设备）70 个，智能设备（物联网终端设备）17 个，操作系统 7 个，安全产品 6 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	228
应用程序	126
网络设备（交换机、路由器等网络端设备）	70
智能设备（物联网终端设备）	17
操作系统	7
安全产品	6
数据库	2

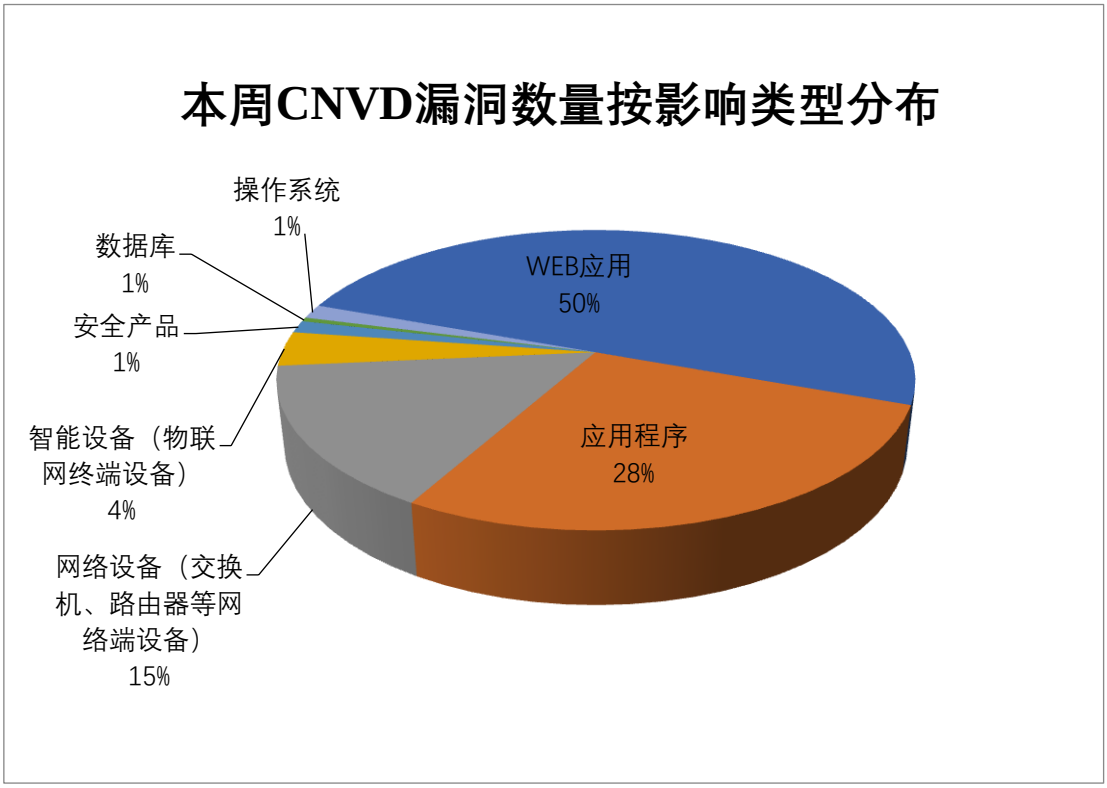

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、恒锋信息科技股份有限公司、FFmpeg 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	22	5%
2	恒锋信息科技股份有限公司	18	4%
3	FFmpeg	13	3%
4	IBM	11	2%
5	PHP Matrimonial Script	10	2%
6	TOTOLINK	10	2%
7	Adobe	10	2%
8	CGAL	8	2%
9	用友网络科技股份有限公司	8	2%
10	其他	346	76%

本周行业漏洞收录情况

本周，CNVD 收录了 52 个电信行业漏洞，13 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“TOTOLINK A720R 存在命令执行漏洞、TOTOLINK A720R 存在二进制漏洞”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/

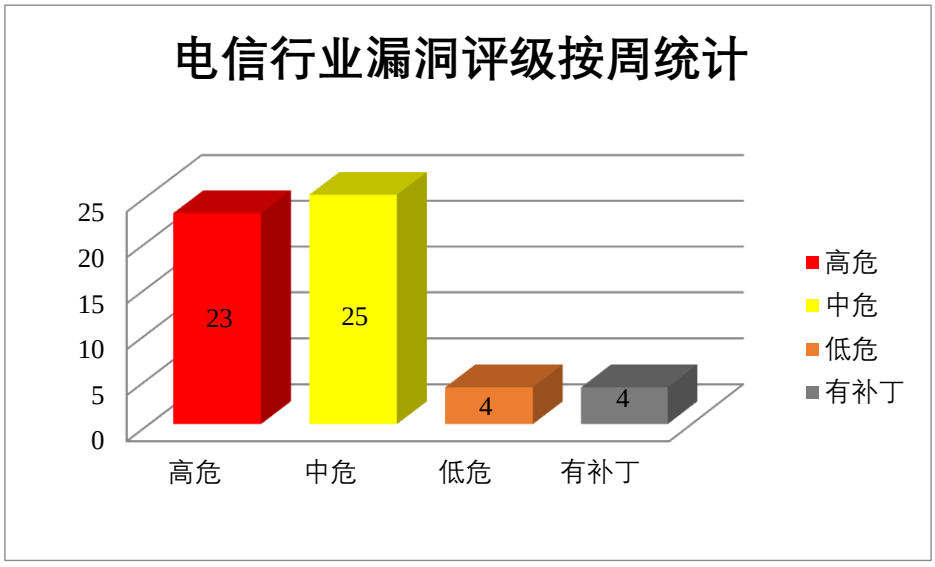

图 3 电信行业漏洞统计

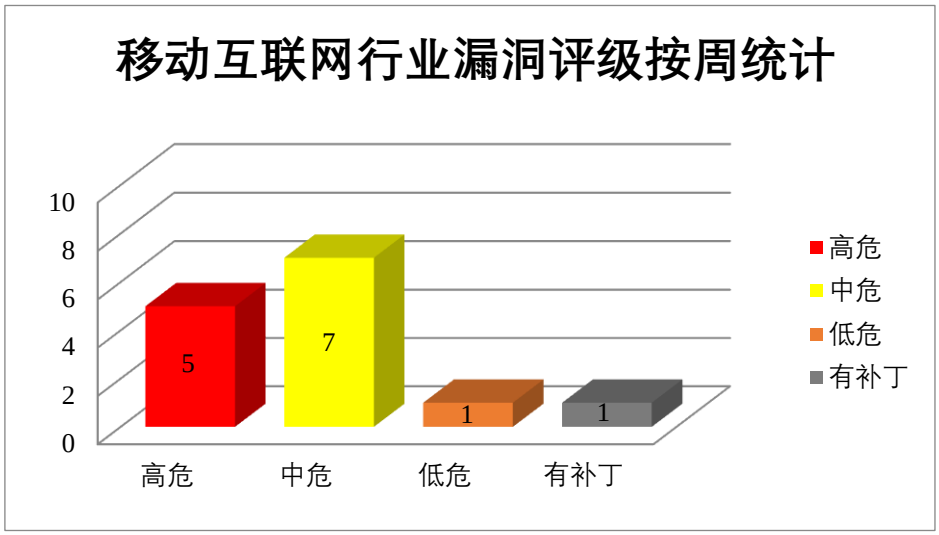

图 4 移动互联网行业漏洞统计

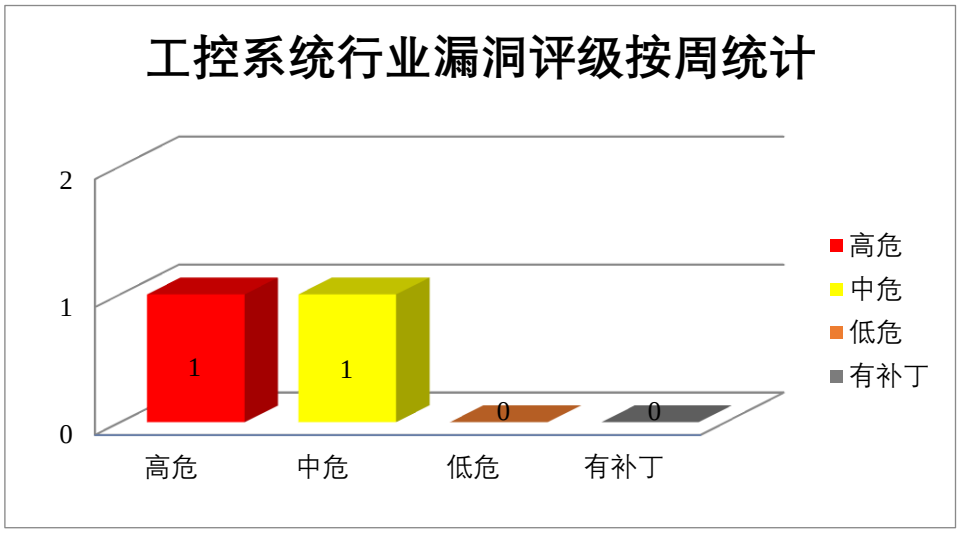

图 5 工控系统行业漏洞统计

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 RoboHelp 是美国奥多比（Adobe）公司的针对 Windows 开发和发布的帮助创作工具。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 Bridge 是 Adobe 公司推出的一款免费数字资产管理应用程序。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，使服务崩溃。

CNVD 收录的相关漏洞包括：Adobe RoboHelp 跨站脚本漏洞（CNVD-2022-60077）、Adobe Photoshop 资源管理错误漏洞（CNVD-2022-60078、CNVD-2022-60076）、Adobe Photoshop 缓冲区溢出漏洞（CNVD-2022-60075）、Adobe Bridge 越界读取漏洞（CN

VD-2022-60081）、Adobe Bridge 内存损坏漏洞、Adobe Bridge 缓冲区溢出漏洞（CNVD-2022-60083、CNVD-2022-60080）。其中，“Adobe Photoshop 资源管理错误漏洞（CNVD-2022-60078、CNVD-2022-60076）”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-2022-60077
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60078
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60076
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60075
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60081
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60079
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60083
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60080

2、IBM 产品安全漏洞

IBM Spectrum Protect 是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。IBM Spectrum Protect（前称 Tivoli Storage Manager）是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。IBM Spectrum Protect Plus 是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。IBM Spectrum Protect Plus 和 IBM Spectrum Copy Data Management 都是美国 IBM 公司的产品。IBM Spectrum Protect Plus 是一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。IBM Spectrum Copy Data Management 是实现数据中心副本管理流程的现代化、简化和自动化。IBM Spectrum Protect Operations Center 是美国 IBM 公司的一个为 IBM Spectrum Protect 环境提供可视化控制的软件。IBM Security Guardium Insights 是美国 IBM 公司的一套数据安全解决方案。该产品支持数据分析、威胁警报、数据安全性审计和本地数据监控等功能。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安全性并获取对易受攻击服务器的未经授权的访问，执行拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM Spectrum Protect 权限提升漏洞（CNVD-2022-60419）、IBM Spectrum Protect 拒绝服务漏洞（CNVD-2022-60417）、IBM Spectrum Protect Server 信息泄露漏洞（CNVD-2022-60413）、IBM Spectrum Protect Plus 信息泄露漏洞（CNVD-2022-60418）、IBM Spectrum Protect Plus 和 IBM Spectrum Copy Data Management 拒绝服务漏洞、IBM Spectrum Protect Plus Container Backup and Restore 权限提升漏洞、IBM Spectrum Protect Operations Center 信息泄露漏洞（CNVD-20

22-60414）、IBM Security Guardium Insights 信息泄露漏洞（CNVD-2022-60422）。其中，“IBM Spectrum Protect 权限提升漏洞（CNVD-2022-60419）”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-2022-60419
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60417
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60413
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60418
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60421
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60416
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60414
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60422

3、Microsoft 产品安全漏洞

Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft .NET Framework 是美国微软（Microsoft）公司的一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。该平台包括 C＃和 Visual Basic 编程语言、公共语言运行库和广泛的类库。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以更高的权限执行任意代码，提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Edge (Chromium-based) 权限提升漏洞（CNVD-2022-60122、CNVD-2022-60121、CNVD-2022-60120、CNVD-2022-60119、CNVD-2022-60118、CNVD-2022-60117、CNVD-2022-60131）、Microsoft .NET Framework 拒绝服务漏洞（CNVD-2022-60136）。其中，“Microsoft .NET Framework 拒绝服务漏洞（CNVD-2022-60136）”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-2022-60122
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60121
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60120
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60119
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60118
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60117
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60131
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60136

4、FFmpeg 产品安全漏洞

FFmpeg 是 Ffmpeg 团队的一套可录制、转换以及流化音视频的完整解决方案。本周，

上述产品被披露存在多个漏洞，攻击者可利用漏洞触发越界读取内存访问，并在系统上执行任意代码，导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：FFmpeg shorten_decode_frame()函数拒绝服务漏洞、FFmpeg rpza_decode_stream()代码执行漏洞、FFmpeg read_var_block_data()函数缓冲区溢出漏洞、FFmpeg msrle_decode_frame()函数拒绝服务漏洞、FFmpeg HEVC video decoder 拒绝服务漏洞、FFmpeg ff_init_buffer_info()函数拒绝服务漏洞、FFmpeg decode_slice_header()函数拒绝服务漏洞（CNVD-2022-60138、CNVD-2022-60145）。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-2022-60139
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60144
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60142
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60140
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60141
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60143
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60138
https://www.cnvd.org.cn/flaw/show/CNVD-2022-60145

5、WAVLINK AERIAL X 1200M 命令注入漏洞

WAVLINK AERIAL X 1200M 是中国 WAVLINK 公司的一款 WiFi 扩展器。本周，WAVLINK AERIAL X 1200M 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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-2022-61031

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-2022-60661	WordPress Hotels/Restaurant/Car Rental Free Booking plugin 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/ecf61d17-8b07-4cb6-93a8-64c2c4fbbe04
CNVD-2022-60129	Microsoft Edge (Chromium-based)篡改漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38669
CNVD-2022	Huawei HarmonyOS 空指针	高	目前厂商已发布升级补丁以修复漏

-61609	漏洞		洞，补丁获取链接：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202207-0000001289909300
CNVD-2022-60667	Google Chrome Intents 安全绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
CNVD-2022-60679	Google Chrome FedCM 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://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
CNVD-2022-60673	GLPI 帮助表单 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://github.com/glpi-project/glpi/security/advisories/GHSA-9q9x-7xxh-w4cg
CNVD-2022-60666	GitLab CE/EE 远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://about.gitlab.com/releases/2022/08/22/critical-security-release-gitlab-15-3-1-released
CNVD-2022-60680	Atlassian Bitbucket Server 和 Data Center 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/BSERV-13438
CNVD-2022-60929	Apache CouchDB 存在命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://apache.org/
CNVD-2022-60419	IBM Spectrum Protect 权限提升漏洞（CNVD-2022-60419）	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.ibm.com/support/pages/node/6564745

小结：本周，Adobe 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，使服务崩溃等。此外，IBM、Microsoft、FFmpeg 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全性并获取对易受攻击服务器的未经授权的访问，执行拒绝服务攻击，以更高的权限执行任意代码，提升权限等。另外，WAVLINK AERIAL X 1200M 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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、 Library Management System SQL 注入漏洞（CNVD-2022-61297）

验证描述

Library Management System 是一个带有二维码考勤和自动生成借书证的图书馆管理系统。

Library Management System 1.0 版本存在 SQL 注入漏洞，该漏洞源于文件/librarian/bookdetails.php 的参数 id 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/CyberThoth/CVE/blob/main/CVE/Library%20Management%20System%20with%20QR%20code%20Attendance/Sql%20Injection/POC.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-61297

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. 葡萄牙国有航空公司 TAP AIR 疑遭 Ragnar Locker 勒索软件攻击

Ragnar Locker 勒索软件团伙声称对葡萄牙的旗舰航空公司 TAP Air Portugal 实施了攻击，该航空公司在其系统于周四（8 月 25 日）晚上遭到攻击后披露上该消息。

参考链接：https://www.secrss.com/articles/46445

2. 图书馆业最大供应商遭勒索软件攻击：系统中断一周多仍未恢复

美国图书馆供应商 Baker & Taylor 公司日前披露，一周前曾遭到勒索软件攻击，目前仍在努力恢复各业务系统。该公司自称是全球最大的图书馆书籍和电子资源分销商。

参考链接：https://www.secrss.com/articles/46441

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