国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 08 月 21 日-2023 年 08 月 27 日　　**2023 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 399 个，其中高危漏洞 208 个、中危漏洞 176 个、低危漏洞 15 个。漏洞平均分值为 6.92。本周收录的漏洞中，涉及 0day 漏洞 271 个（占 68%），其中互联网上出现“Milesight UR32L zebra vlan_name 功能命令执行漏洞、emlog 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 17404 个，与上周（22602 个）环比减少 23%。

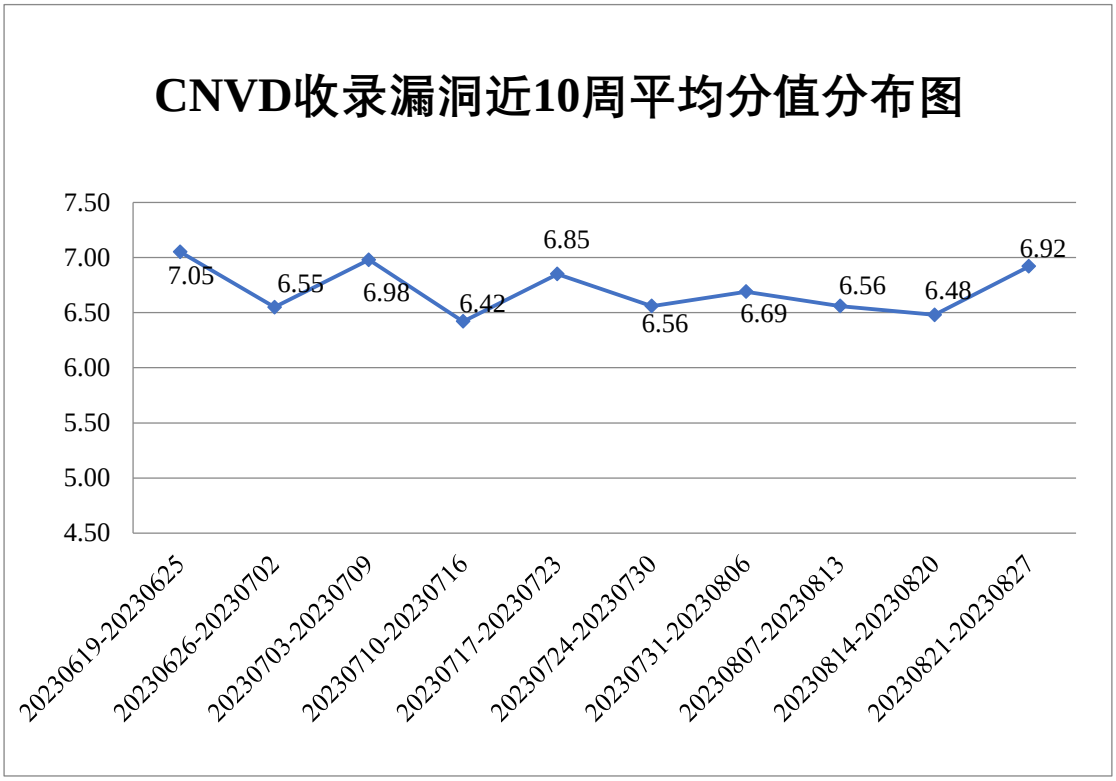

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向基础电信企业通报漏洞事件 6 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 721 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 84 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 23 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：

字节跳动安全中心、珠海金山办公软件有限公司、重庆知翰合众科技有限公司、重庆市綦江区城市建设投资有限公司、重庆升话宝信息科技有限公司、重庆猫扑网络科技有限公司、中新网络信息安全股份有限公司、中出行科技集团（河南）有限公司、中保科技集團、郑州微厦计算机科技有限公司、浙江职信通信科技有限公司、浙江鸿星文具有限公司、浙江好络维医疗技术有限公司、掌如科技服务有限公司、长沙冉星信息科技有限公司、云之家网络（重庆）有限公司、昱能科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易如意、阳光电源股份有限公司、信呼、新云网科技集团股份有限公司、新天科技股份有限公司、新开普电子股份有限公司、夏普科技（上海）有限公司、西安华谊云信息科技有限公司、武汉烽火信息集成技术有限公司、无锡信捷电气股份有限公司、卫宁健康科技集团股份有限公司、潍坊家园驿站电子技术有限公司、微软（中国）有限公司、网是科技股份有限公司、万通 CMS、天津天堰科技股份有限公司、天地（常州）自动化股份有限公司、台达集团、四川迅睿云软件开发有限公司、四川奇石缘科技股份有限公司、四川海底捞餐饮股份有限公司、曙光信息产业股份有限公司、施耐德电气（中国）有限公司、昇频股份有限公司、深圳坐标软件集团有限公司、深圳智慧光迅信息技术有限公司、深圳市亿图软件有限公司、深圳市设施之家科技有限公司、深圳市跨境伙伴网络科技有限公司、深圳市酷瓜软件有限公司、深圳市科脉技术股份有限公司、深圳市精农富仓农业有限公司、深圳市吉祥腾达科技有限公司、深圳深知未来智能有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海瑞美信息技术有限公司、上海穆云智能科技有限公司、上海秒优供应链管理有限公司、上海寰创通信科技股份有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海布雷德科技有限公司、山西风行测控股份有限公司、山东云时空信息科技有限公司 、山东潍大软件有限公司、山东大有医网医疗科技有限公司、山东博硕自动化技术有限公司、山东比特智能科技股份有限公司、厦门星纵物联科技有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、普联技术有限公司、南宁火蝶科技有限公司、南京先极科技有限公司、南昌蓝智科技有限公司、绿盟科技集团股份有限公司、漯河市大有前途网络科技有限公司、洛阳云业信息科技有限公司、领航未来（北京）科技有限公司、联想集团、乐荐健康科技集团有限公司、浪潮通用软件有限公司、江西铭软科技有限公司、江苏有线邦联新媒体科技有限公司、江苏优

度软件有限公司、江苏九一网络科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、华科网络技术开发、弘扬软件股份有限公司、弘成科技发展有限公司、河北中废通拍卖有限公司、杭州易软共创网络科技有限公司、杭州叙简科技股份有限公司、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、杭州九麒科技有限公司、杭州今奥信息科技股份有限公司、杭州海康威视数字技术股份有限公司、海南翼智慧信息科技有限公司、哈尔滨伟成科技有限公司、国交信息股份有限公司、贵州觅新科技有限公司、广州图创计算机软件开发有限公司、广州思迈特软件有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东飞企互联科技股份有限公司、富士胶片商业创新（中国）有限公司、福建科立讯通信有限公司、菲尼克斯（中国）投资有限公司、顶点软件股份有限公司、帝国软件、成都双流阿如拉互联网医院有限公司、成都佳海信通网络技术有限公司、成都飞鱼星科技股份有限公司、成都铂贝科技有限公司、畅捷通信息技术股份有限公司、沧州市新星传媒、北京中科金马科技股份有限公司、北京致远互联软件股份有限公司、北京长亭未来科技有限公司、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、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京网康科技有限公司、北京通宇泰克科技股份有限公司、北京通达信科科技有限公司、北京硕人时代科技股份有限公司、北京数码视讯科技股份有限公司、北京欧倍尔软件技术开发有限公司、北京朗新天霁软件技术有限公司、北京昆仑亿发科技股份有限公司、北京金盘鹏图软件技术有限公司、北京金和网络股份有限公司、北京国通创安报警网络技术有限公司、北京辰信领创信息技术有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、百度安全应急响应中心、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽共生物流科技有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心、ZZCMS、YYCMS、SpringBootCMS、Sercomm、SEMCMS、RPCMS、jrecms 和 Dreamer CMS。

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、北京神州绿盟科技有限公司、新华三技术有限公司、安天科技集团股份有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。联想集团、重庆电信系统集成有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、安徽锋刃信息科技有限公司、陕西慧缘网络科技有限公司、河南灵创电子科技有限公司、亚信科技（成都）有限公司、浙江中控技术股份有限公司、杭州海康威视数字技术股份有限公司、河南信安世纪科技有限公司、赛尔网络有限公司、博智安全科技股份有限公司、苏州棱镜七彩信息科技有限公司、超聚变数字技术有限公司、北京微步在线科技有限公司、智网安云（武汉）信息技术有限公司、贵州泰若数字科技有限公司、北京君云天下科技有限公司、山

东正中信息技术股份有限公司（SDZZ-01）、深圳昂楷科技有限公司、汇安云（山东）信息科技有限公司、工业和信息化部电子第五研究所、郑州埃文计算机科技有限公司、任子行网络技术股份有限公司、郑州师范学院、浙江东安检测技术有限公司、广州安亿信软件科技有限公司、南京深安科技有限公司、信息产业信息安全测评中心、深圳市魔方安全科技有限公司、北京水木羽林科技有限公司、成都泰瑞通信设备检测有限公司、南方电网数字电网集团信息通信科技有限公司、江苏晟晖信息科技有限公司、中国电信股份有限公司上海研究院、广州市盛通建设工程质量检测有限公司及其他个人白帽子向 CNVD 提交了 17404 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、三六零数字安全科技集团有限公司和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 15914 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）	14723	14723
上海交大	718	718
北京启明星辰信息安全技术有限公司	400	4
北京神州绿盟科技有限公司	296	7
新华三技术有限公司	262	0
三六零数字安全科技集团有限公司	255	255
安天科技集团股份有限公司	232	0
奇安信网神（补天平台）	218	218
深信服科技股份有限公司	214	16
北京天融信网络安全技术有限公司	128	5
阿里云计算有限公司	95	0
北京数字观星科技有限公司	83	0
天津市国瑞数码安全系统股份有限公司	66	0
北京知道创宇信息技	46	0

术有限公司		
杭州安恒信息技术股份有限公司	44	25
杭州迪普科技股份有限公司	25	0
北京智游网安科技有限公司	3	3
华为技术有限公司	2	2
联想集团	112	112
重庆电信系统集成有限公司	45	45
快页信息技术有限公司	33	33
河南东方云盾信息技术有限公司	31	31
安徽锋刃信息科技有限公司	24	24
陕西慧缘网络科技有限公司	8	8
河南灵创电子科技有限公司	7	7
亚信科技（成都）有限公司	6	6
浙江中控技术股份有限公司	6	6
杭州海康威视数字技术股份有限公司	4	4
河南信安世纪科技有限公司	4	4
赛尔网络有限公司	3	3
博智安全科技股份有限公司	3	3
苏州棱镜七彩信息科技有限公司	2	2
超聚变数字技术有限	2	2

公司		
北京微步在线科技有限公司	2	2
智网安云（武汉）信息技术有限公司	2	2
贵州泰若数字科技有限公司	2	2
北京君云天下科技有限公司	2	2
山东正中信息技术股份有限公司（SDZZ-01）	2	2
深圳昂楷科技有限公司	2	2
汇安云（山东）信息科技有限公司	2	2
工业和信息化部电子第五研究所	2	2
郑州埃文计算机科技有限公司	2	2
任子行网络技术股份有限公司	1	1
郑州师范学院	1	1
浙江东安检测技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
南京深安科技有限公司	1	1
信息产业信息安全测评中心	1	1
深圳市魔方安全科技有限公司	1	1
北京水木羽林科技有限公司	1	1

成都泰瑞通信设备检测有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
江苏晟晖信息科技有限公司	1	1
中国电信股份有限公司上海研究院	1	1
广州市盛通建设工程质量检测有限公司	1	1
CNCERT 广西分中心	1	1
个人	1106	1106
报送总计	19238	17404

本周漏洞按类型和厂商统计

本周，CNVD 收录了 399 个漏洞。WEB 应用 165 个，应用程序 99 个，网络设备（交换机、路由器等网络端设备）96 个，操作系统 20 个，数据库 9 个，智能设备（物联网终端设备）6 个，安全产品 4 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	165
应用程序	99
网络设备（交换机、路由器等网络端设备）	96
操作系统	20
数据库	9
智能设备（物联网终端设备）	6
安全产品	4

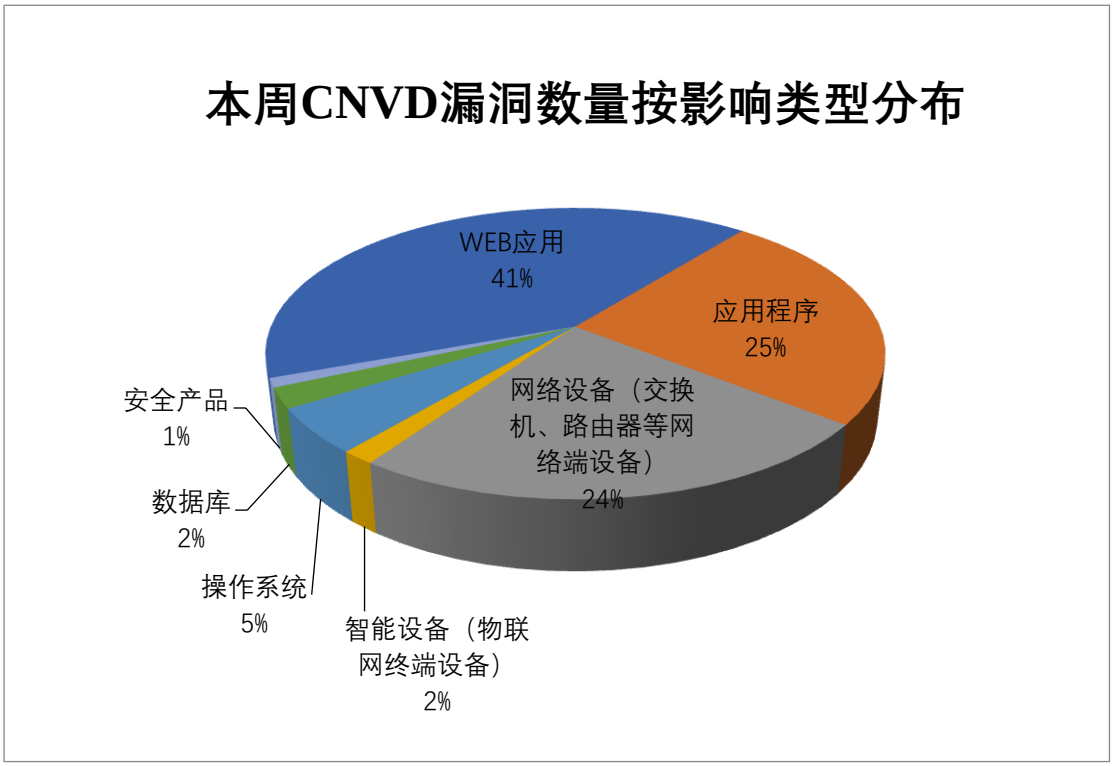

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 MileSight、Microsoft、NETGEAR 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	MileSight	37	9%
2	Microsoft	20	5%
3	NETGEAR	11	3%
4	Moxa	11	3%
5	ChurchCRM	10	2%
6	IBM	9	2%
7	Huawei	8	2%
8	北京通达信科科技有限公司	6	2%
9	用友网络科技股份有限公司	6	2%
10	其他	281	70%

本周行业漏洞收录情况

本周，CNVD 收录了 80 个电信行业漏洞，29 个移动互联网行业漏洞，6 个工控行

业漏洞（如下图所示）。其中，“MOXA TN-4900 and TN-5900 命令注入漏洞、Rockwell Automation ThinManager 路径遍历漏洞（CNVD-2023-64278）、NETGEAR XR300 缓冲区溢出漏洞”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/

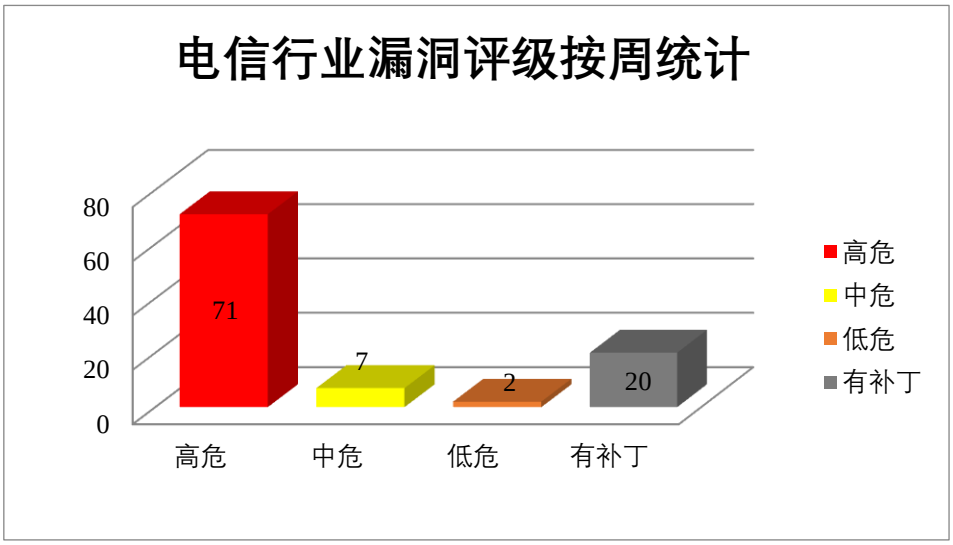

图 3 电信行业漏洞统计

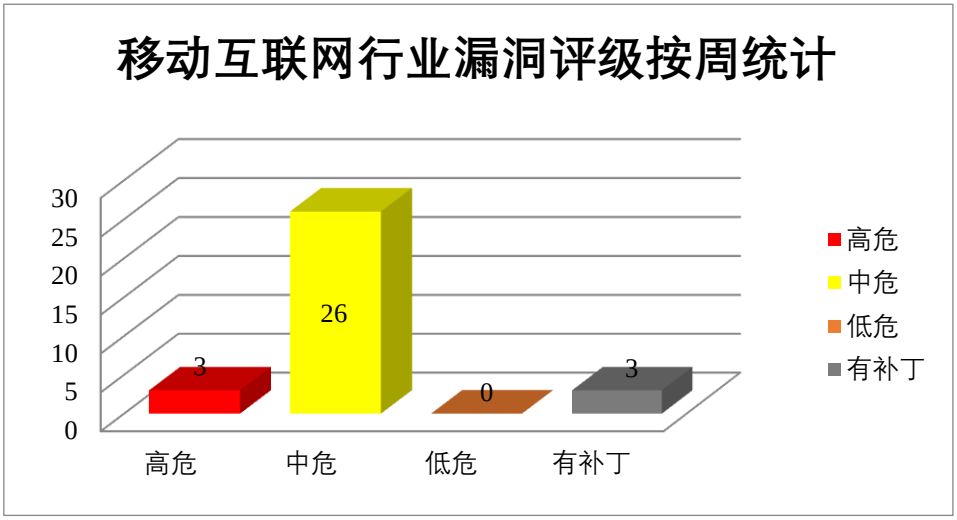

图 4 移动互联网行业漏洞统计

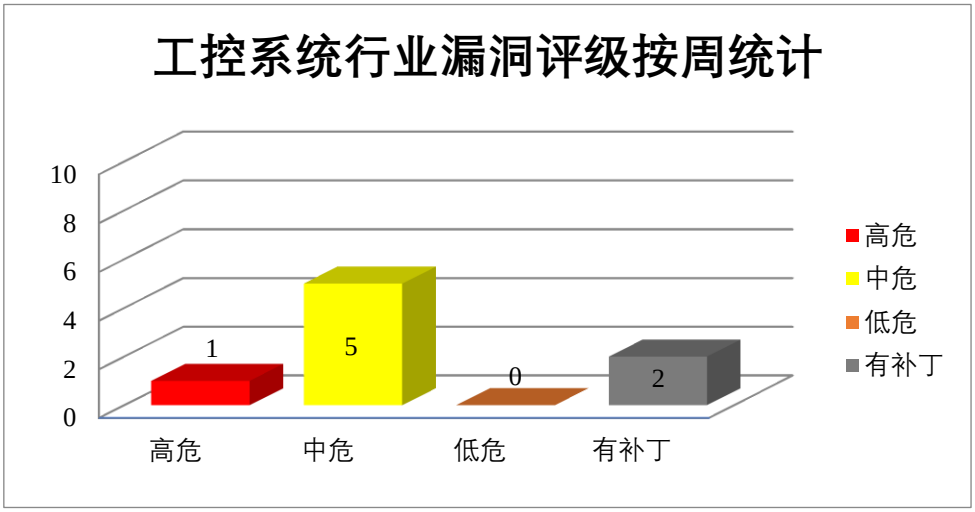

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Microsoft HEVC Video Extensions 是美国微软（Microsoft）公司的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。Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Excel 远程代码执行漏洞（CNVD-2023-64864）、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2023-64865、CNVD-2023-64867、CNVD-2023-64868）、Microsoft Exchange Server 权限提升漏洞（CNVD-2023-64869）、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2023-64870）、Microsoft SharePoint Server 欺骗漏洞（CNVD-2023-64872、CNVD-2023-64873）。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-2023-64864

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64865

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64867

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64868

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64869

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64870

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64872

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64873

2、MOXA 产品安全漏洞

MOXA TN-4900 是中国摩莎（MOXA）公司的一系列工业防火墙路由器。MOXA TN-5900 是中国摩莎（MOXA）公司的一系列工业防火墙路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞删除任意文件，在受影响的设备上执行远程代码等。

CNVD 收录的相关漏洞包括：MOXA TN-4900 and TN-5900 命令注入漏洞（CNVD-2023-64095、CNVD-2023-64094、CNVD-2023-64098、CNVD-2023-64097、CNVD-2023-64096）、MOXA TN-5900 命令注入漏洞（CNVD-2023-64100、CNVD-2023-64099）、MOXA TN-5900 身份验证错误漏洞。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-2023-64095

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64094

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64098

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64097

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64096

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64100

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64099

https://www.cnvd.org.cn/flaw/show/CNVD-2023-64214

3、NETGEAR 产品安全漏洞

NETGEAR R7100LG 是美国网件（NETGEAR）公司的一款路由器。连接两个或多个网络的硬件设备，在网络间起网关的作用。NETGEAR R6900P 是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR EX6200 是美国网件（NETGEAR）公司的一款无线网络信号扩展器。NETGEAR DG834Gv5 是美国网件（NETGEAR）公司的一款无线 ADSL 防火墙调制解调器。NETGEAR RBR750 是美国网件（NETGEAR）公司的一套家庭 WiFi 系统。Netgear R6250 是 Netgear 公司推出的一款路由器。NETGEAR XR300 是美国网件（NETGEAR）公司的一款无线路由器。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者导致拒绝服务。

CNVD 收录的相关漏洞包括：NETGEAR R7100LG 命令注入漏洞、NETGEAR R6900P 缓冲区溢出漏洞、NETGEAR EX6200 缓冲区溢出漏洞、NETGEAR DG834Gv5 缓冲区溢出漏洞、NETGEAR RBR750 命令注入漏洞、NETGEAR RBR750 dev_name

参数命令注入漏洞、Netgear R6250 命令注入漏洞、NETGEAR XR300 缓冲区溢出漏洞。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-2023-64072
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64071
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64070
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64068
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64076
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64075
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64074
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64073

4、IBM 产品安全漏洞

IBM DB2 是美国国际商业机器（IBM）公司的一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞代码执行，导致拒绝服务。

CNVD 收录的相关漏洞包括：IBM DB2 拒绝服务漏洞（CNVD-2023-64876、CNVD-2023-64877、CNVD-2023-64878、CNVD-2023-64879、CNVD-2023-64880、CNVD-2023-64881、CNVD-2023-64882）、IBM DB2 代码执行漏洞（CNVD-2023-64883）。其中，除“IBM DB2 拒绝服务漏洞（CNVD-2023-64881）”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-2023-64876
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64877
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64878
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64879
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64880
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64881
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64882
https://www.cnvd.org.cn/flaw/show/CNVD-2023-64883

5、TeleAdapt RoomCast TA-2400 权限提升漏洞

TeleAdapt RoomCast TA-2400 是英国 TeleAdapt 公司的一款适用于客房的一体化、自带的顶级内容流媒体盒。本周，TeleAdapt RoomCast TA-2400 被披露存在权限提升漏洞。该漏洞是由于 Android Debug Bridge（ADB）的访问控制不当造成的。攻击者可利用该漏洞获得提升的 root 权限。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-2023-64884

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：https://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-2023-64085	Zyxel NBG6604 命令注入漏洞（CNVD-2023-64085）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-in-ntp-feature-of-nbg6604-home-router
CNVD-2023-64092	Huawei HarmonyOS 越界写入漏洞（CNVD-2023-64092）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725
CNVD-2023-64278	Rockwell Automation ThinManager 路径遍历漏洞（CNVD-2023-64278）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/magic-post-thumbnail/#developers
CNVD-2023-64277	ASUSTOR Data Master 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://launchpad.support.sap.com/#/notes/3315312
CNVD-2023-64505	Adobe Dimension 释放后重用漏洞	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/dimension/apsb23-44.html
CNVD-2023-64637	WordPress Booking Manager plugin 服务端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/booking-manager/
CNVD-2023-64814	WinRAR 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://www.win-rar.com/start.html?&L=7
CNVD-2023-64853	Smartbi windowUnloading 身份认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.smartbi.com.cn/patchinfo
CNVD-2023	F5 BIG-IP 操作系统命令注	高	厂商已发布了漏洞修复程序，请及

-65132	入漏洞		时关注更新：https://my.f5.com/manage/s/article/K000132972
CNVD-2023-65131	emlog 代码问题漏洞（CNVD-2023-65131）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/emlog/emlog/releases

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，提升权限，在系统上执行任意代码。此外，MOXA、NETGEAR、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞删除任意文件，在系统上执行任意代码或者导致拒绝服等。另外，TeleAdapt RoomCast TA-2400 被披露存在权限提升漏洞。攻击者可利用该漏洞获得提升的 root 权限。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、Milesight UR32L zebra vlan_name 功能命令执行漏洞

验证描述

Milesight UR32L 是中国星纵物联（Milesight）公司的一个 4G 工业路由器。

Milesight UR32L zebra vlan_name 功能存在命令执行漏洞，攻击者可利用该漏洞在系统上执行任意命令。

验证信息

POC 链接：https://talosintelligence.com/vulnerability_reports/TALOS-2023-1723

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-64960

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. Ivanti 曝新的 MobileIron 零日漏洞，正在被恶意利用

网络安全公司 mnemonic 的研究人员发现并报告了这个零日漏洞（CVE-2023-38035），未经身份验证的攻击者可以通过 MobileIron 配置服务（MICS）使用的 8443 端口访问敏感的管理门户配置 API。攻击者利用限制性不足的 Apache HTTPD 配置绕过身份验证控

制后，就可以实现这一点。

参考链接：https://www.freebuf.com/news/375839.html

2. TP-Link 智能灯泡漏洞曝光，用户 WiFi 密码易被窃取

研究人员近日在 TP-Link Tapo L530E 智能灯泡和 TP-Link Tapo 应用程序中发现了 4 个漏洞，攻击者可以利用这些漏洞窃取目标的 WiFi 密码。

参考链接：http://www.anquan419.com/knews/24/5747.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