国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 10 月 09 日-2023 年 10 月 15 日 **2023 年第 41 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 352 个，其中高危漏洞 177 个、中危漏洞 159 个、低危漏洞 16 个。漏洞平均分值为 6.48。本周收录的漏洞中，涉及 0day 漏洞 276 个（占 78%），其中互联网上出现“TOTOLINK A3002R 缓冲区溢出漏洞、PortlandLabs Concrete CMS SEO-Extra 功能跨站脚本漏洞”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 19726 个，与上周（10321 个）环比增加 91%。

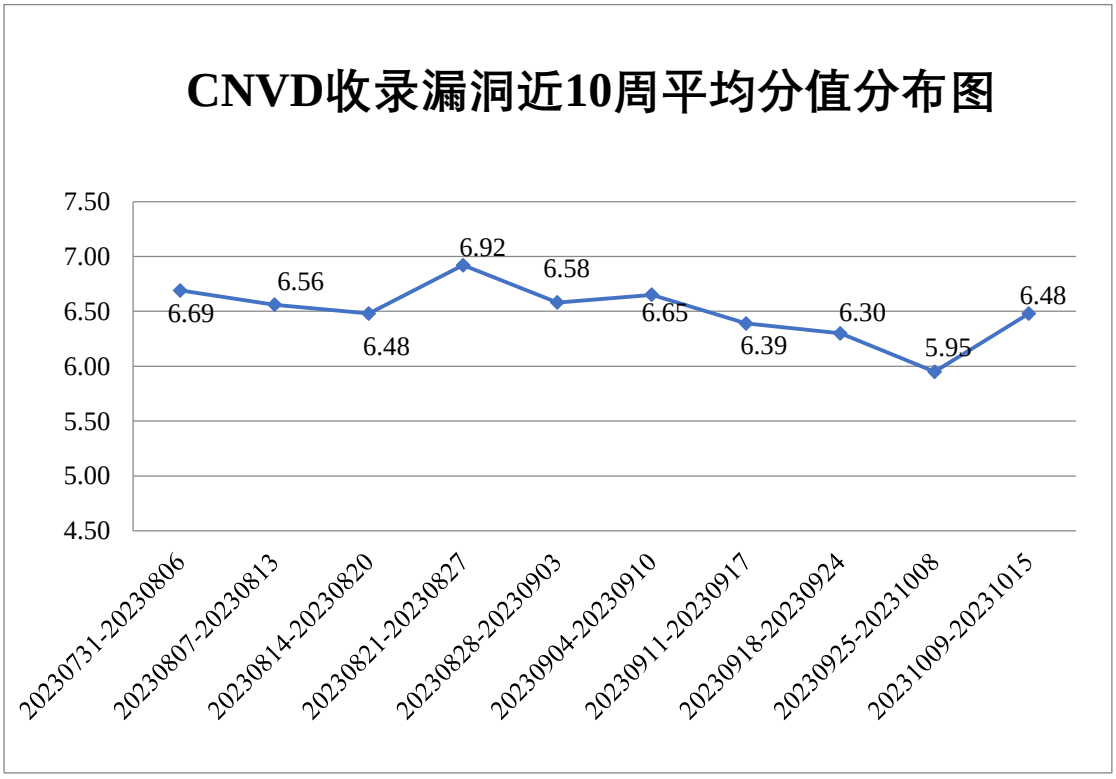

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 14 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 1126 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 278 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 82 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：

紫光股份有限公司、淄博闪灵网络科技有限公司、重庆中联信息产业有限责任公司、重庆医美之恋科技有限责任公司、中通云仓科技有限公司、中科数字通（北京）科技有限公司、中科方德软件有限公司、中孚信息股份有限公司、智达信科技术股份有限公司、浙江浙大网新国际软件技术服务有限公司、浙江宇视科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江哈罗鱼科技有限公司、长沙健海思远科技有限公司、云南链滴科技有限公司、友讯电子设备（上海）有限公司、友帮信互联网技术（北京）有限公司、用友网络科技股份有限公司、永春县永源城市建设有限公司、盈嘉互联（北京）科技有限公司、星软集团有限公司、信也科技集团、心动网络股份有限公司、小米科技有限责任公司 、小白智能科技（长春）股份有限公司、夏普商贸（中国）有限公司、西安炎燚信息科技有限公司、西安启莱软件科技有限公司、武汉达梦数据库股份有限公司、五代（武汉）科技有限公司、网件公司、同望科技股份有限公司、天津天堰科技股份有限公司、特斯拉（上海）有限公司、唐山市柳林自动化设备有限公司、苏州真趣信息科技有限公司、苏州摩多多信息科技有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、世邦通信股份有限公司、时尚致爱（北京）文化有限公司、沈阳乐在途中旅游服务有限公司、深圳市一应科技有限公司、深圳市微耕实业有限公司、深圳市美科星通信技术有限公司、深圳市科荣软件股份有限公司、深圳市科脉技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市富士智能股份有限公司、深圳市弗格远有限公司、深圳市道尔智控科技股份有限公司、深圳市宝泽科技有限公司、深圳齐心好视通云计算有限公司、深圳弘恒发展控股集团有限公司、深圳昂楷科技有限公司、绍兴多米网络科技有限公司、上海卓卓网络科技有限公司、上海装盟信息科技有限公司、上海甄云信息科技有限公司、上海逸尚云联信息技术股份有限公司、上海雅高文化传播有限公司、上海新晗网络科技有限公司、上海三高计算机中心股份有限公司、上海企望信息科技有限公司、上海普华科技发展股份有限公司、上海哪吒聚行信息科技技术有限公司、上海穆云智能科技有限公司、上海肯特仪表股份有限公司、上海九方云智能科技有限公司、上海恒企专修学院有限公司、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、上海二三四五移动科技有限公司、上海顶想信息科技有限公司、上海博达数据通信有限公司、上海爱数信息技术股份有限公司、陕西

小伙伴网络科技有限公司、陕西西泰环保科技有限公司、山西联康科技有限公司、厦门信昇达物联科技有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、清枫（北京）科技有限公司、青岛雨诺网络信息股份有限公司、普联技术有限公司、鹏为软件股份有限公司、欧德神思软件系统（北京）有限公司、南宁凡享网络科技有限公司、南京数旗科技有限公司、联想（北京）有限公司、浪潮通用软件有限公司、廊坊市极致网络科技有限公司、蓝卓数字科技有限公司、辣苹果网络技术（大连）有限公司、九一到家（北京）科技有限公司、京瓷办公设备科技（东莞）有限公司、金华市宁志网络科技有限公司、鉴正宝信息技术有限公司、嘉兴想天信息科技有限公司、济南宏之博信息技术有限公司、济南爱程网络科技有限公司、吉翁电子（深圳）有限公司、吉林省美满婚姻服务有限公司、基恩士（中国）有限公司、华润万家（控股）有限公司、湖南众合百易信息技术有限公司、湖南壹拾捌号网络技术有限公司、黑龙江储饲粮农业科技集团有限公司、河北咱家健康软件科技有限公司、杭州言商网络技术有限公司、杭州小麦互动科技有限公司、杭州先锋电子技术股份有限公司、杭州摩的科技有限公司、杭州蚂蚁上数信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、杭州爱尚租租网络科技有限公司、广州小鹿信息技术有限责任公司、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、广州市起秀信息科技有限公司、广州市大象飞信息科技有限公司、广州艮业信息科技有限公司、广西浪潮国强软件有限公司、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、福清市云黑网络科技有限公司、福建省海峡信息技术有限公司、飞友科技有限公司、东华软件股份公司、东方网力科技股份有限公司、鼎捷软件股份有限公司、大连富豪科技有限公司、创业慧康科技股份有限公司、成都零起飞科技有限公司、北京中思远信息科学研究院、北京致远互联软件股份有限公司、北京正影网络科技有限公司、北京英华在线科技有限公司、北京亿赛通科技发展有限责任公司、北京一轻食品集团有限公司、北京星网锐捷网络技术有限公司、北京象新力科技有限公司、北京微瑞集智科技有限公司、北京万讯博通科技发展有限公司、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京硕人时代科技股份有限公司、北京数字政通科技股份有限公司、北京世间万象网络科技有限公司、北京世纪明德教育科技股份有限公司、北京世纪超星信息技术发展有限责任公司、北京神州数码云科信息技术有限公司、北京尚洋东方环境科技有限公司、北京睿智博创科技有限公司、北京派网软件有限公司、北京妙音数科股份有限公司、北京龙软科技股份有限公司、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、北京火山引擎科技有限公司、北京国通创安报警网络技术有限公司、北京高速波软件有限公司、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、北京百朋索奇科技有限公司、北京百度网讯科技有限公司、北京安盟信息技术股份有限公司、北京安博通科技股份有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心、ZZCMS、zbzcms、SEMCMS 和 Adobe。

本周，CNVD 发布了《F5 发布 2023 年 10 月季度安全通告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9361

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、天津市国瑞数码安全系统股份有限公司、新华三技术有限公司、安天科技集团股份有限公司、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、杭州美创科技有限公司、亚信科技（成都）有限公司、中孚安全技术有限公司、安徽锋刃信息科技有限公司、快页信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、湖南泛联新安信息科技有限公司、合肥梆梆信息科技有限公司、赛尔网络有限公司、西藏熙安信息技术有限责任公司、北京君云天下科技有限公司、江苏天竞云合数据技术有限公司、江苏晟晖信息科技有限公司、杭州默安科技有限公司、博智安全科技股份有限公司、北京水木羽林科技有限公司、河南灵创电子科技有限公司、江西和尔惠信息技术有限公司、河南东方云盾信息技术有限公司、国网江西省电力有限公司电力科学研究院、浙江中控技术股份有限公司、广州安亿信软件科技有限公司、北京微步在线科技有限公司、工业和信息化部电子第五研究所-数据治理服务中心、神州灵云（北京）科技有限公司、广东拓思软件科学园有限公司、浙江东安检测技术有限公司、北京山石网科信息技术有限公司、上海直画科技有限公司、北京远禾科技有限公司、广东盈世计算机科技有限公司、超聚变数字技术有限公司、江苏君立华域信息安全技术股份有限公司、山东云天安全技术有限公司、苏州棱镜七彩信息科技有限公司、南京师范大学常州创新发展研究院软件与信息安全测评中心、平安银河实验室、河南悦海数安科技有限公司、信息产业信息安全测评中心、成都天天网安信息安全技术有限公司、郑州埃文计算机科技有限公司、广西网信信息技术有限公司、北京威努特技术有限公司、江苏极元信息技术有限公司、北方实验室（沈阳）股份有限公司、陕西慧缘网络科技有限公司、华润数科控股有限公司、江西诚韬科技有限公司、上海谋乐网络科技有限公司、北京天防安全科技有限公司、北京双湃智安科技有限公司及其他个人白帽子向 CNVD 提交了 19726 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）、斗象科技（漏洞盒子）、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 17551 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）	14424	14424

斗象科技（漏洞盒子）	2351	2351
北京天融信网络安全技术有限公司	1068	0
天津市国瑞数码安全系统股份有限公司	943	0
新华三技术有限公司	886	0
上海交大	535	535
安天科技集团股份有限公司	330	0
深信服科技股份有限公司	263	16
三六零数字安全科技集团有限公司	241	241
北京数字观星科技有限公司	136	0
阿里云计算有限公司	132	6
杭州安恒信息技术股份有限公司	82	3
北京知道创宇信息技术有限公司	76	0
北京神州绿盟科技有限公司	68	1
杭州迪普科技股份有限公司	29	1
中电科网络安全科技股份有限公司	23	23
南京联成科技发展股份有限公司	7	7
中国电信集团系统集成有限责任公司	7	7
北京启明星辰信息安全技术有限公司	4	4
北京升鑫网络科技有限公司（青藤云）	2	2
北京智游网安科技有	2	2

限公司		
浙江大华技术股份有限公司	2	2
远江盛邦（北京）网络安全科技股份有限公司	2	2
华为技术有限公司	1	1
贵州泰若数字科技有限公司	1	1
联想集团	175	175
杭州美创科技有限公司	75	75
亚信科技（成都）有限公司	72	72
中孚安全技术有限公司	61	61
安徽锋刃信息科技有限公司	39	39
快页信息技术有限公司	30	30
奇安星城网络安全运营服务（长沙）有限公司	25	25
F5	23	0
西门子（中国）有限公司	21	0
湖南泛联新安信息科技有限公司	19	19
合肥梆梆信息科技有限公司	18	18
赛尔网络有限公司	9	9
西藏熙安信息技术有限责任公司	7	7
北京君云天下科技有限公司	7	7

江苏天竞云合数据技术有限公司	7	7
江苏晟晖信息科技有限公司	7	7
杭州默安科技有限公司	7	7
博智安全科技股份有限公司	6	6
北京水木羽林科技有限公司	5	5
河南灵创电子科技有限公司	5	5
江西和尔惠信息技术有限公司	4	4
河南东方云盾信息技术有限公司	4	4
国网江西省电力有限公司电力科学研究院	3	3
浙江中控技术股份有限公司	3	3
广州安亿信软件科技有限公司	3	3
北京微步在线科技有限公司	3	3
工业和信息化部电子第五研究所-数据治理服务中心	2	2
神州灵云（北京）科技有限公司	2	2
广东拓思软件科学园有限公司	2	2
浙江东安检测技术有限公司	2	2
北京山石网科信息技术有限公司	2	2

上海直画科技有限公司	2	2
北京远禾科技有限公司	2	2
广东盈世计算机科技有限公司	2	2
超聚变数字技术有限公司	2	2
江苏君立华域信息安全技术股份有限公司	2	2
山东云天安全技术有限公司	2	2
苏州棱镜七彩信息科技有限公司	1	1
南京师范大学常州创新发展研究院软件与信息安全测评中心	1	1
平安银河实验室	1	1
河南悦海数安科技有限公司	1	1
信息产业信息安全测评中心	1	1
成都天天网安信息安全技术有限公司	1	1
郑州埃文计算机科技有限公司	1	1
广西网信信息技术有限公司	1	1
北京威努特技术有限公司	1	1
江苏极元信息技术有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
陕西慧缘网络科技有	1	1

限公司		
华润数科控股有限公司	1	1
江西诚韬科技有限公司	1	1
上海谋乐网络科技有限公司	1	1
北京天防安全科技有限公司	1	1
北京双湃智安科技有限公司	1	1
CNCERT 宁夏分中心	8	8
CNCERT 河北分中心	2	2
CNCERT 广西分中心	1	1
CNCERT 贵州分中心	1	1
个人	1452	1452
报送总计	23756	19726

本周漏洞按类型和厂商统计

本周，CNVD 收录了 352 个漏洞。WEB 应用 235 个，应用程序 70 个，网络设备（交换机、路由器等网络端设备）29 个，操作系统 12 个，安全产品 5 个，车联网 1 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	235
应用程序	70
网络设备（交换机、路由器等网络端设备）	29
操作系统	12
安全产品	5
车联网	1

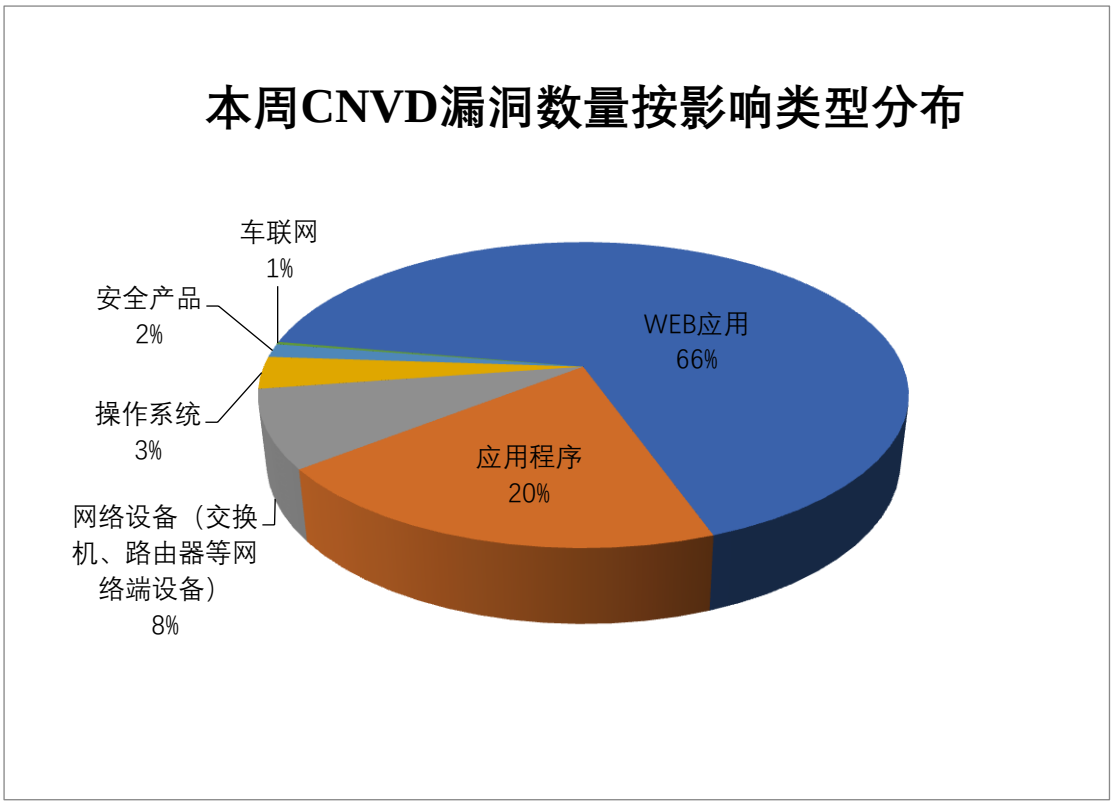

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Google、F5 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	Siemens	21	6%
2	Google	20	6%
3	F5	16	5%
4	Mozilla	10	3%
5	Microsoft	8	2%
6	红色婚纱摄影模板	7	2%
7	用友网络科技股份有限公司	7	2%
8	郸城县新翔软件科技有限公司	5	1%
9	嘉兴想天信息科技有限公司	5	1%
10	其他	253	72%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，47 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，“Siemens Tecnomatix Plant Simulation 文件分析漏洞、Google Android 权限提升漏洞（CNVD-2023-75544）、Siemens SICAM A8000 设备 CP CI85 固件 Web 服务器路径遍历漏洞”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/

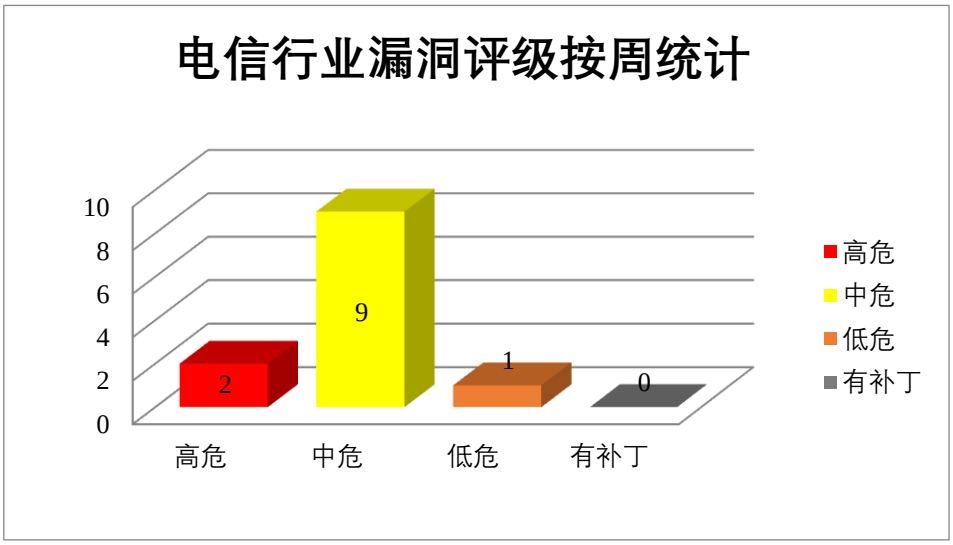

图 3 电信行业漏洞统计

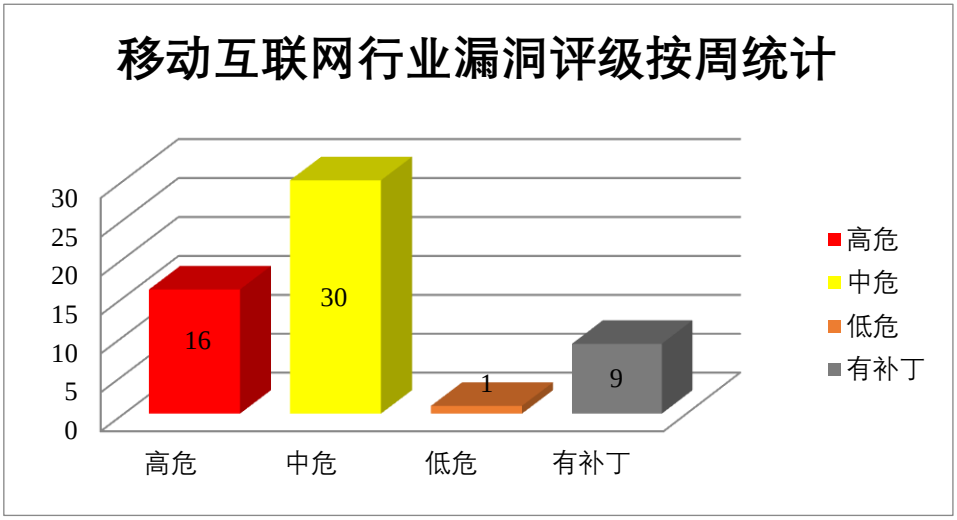

图 4 移动互联网行业漏洞统计

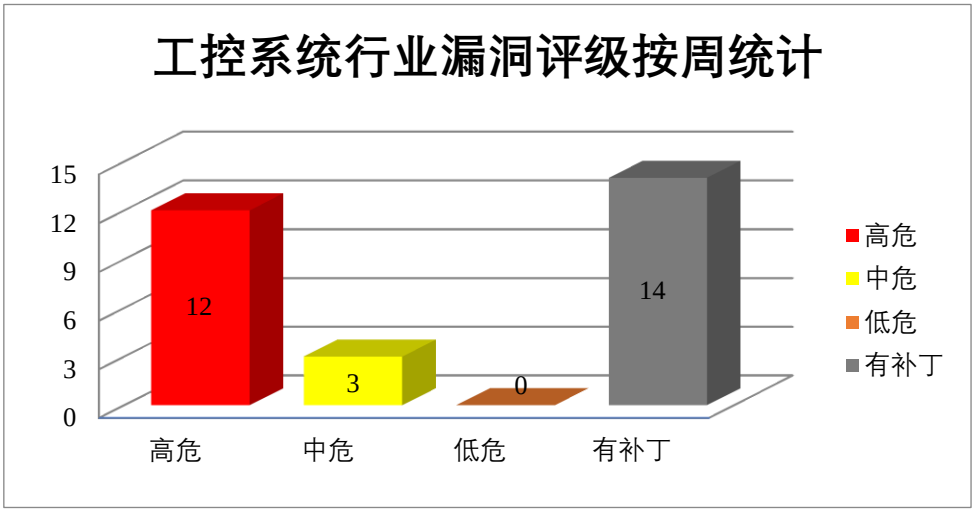

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上运行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-75536、CNVD-2023-75537、CNVD-2023-75539、CNVD-2023-75540、CNVD-2023-75541、CNVD-2023-75543、CNVD-2023-75544）、Google Android 代码执行漏洞（CNVD-2023-75542）。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-2023-75536
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75537
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75539
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75540
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75541
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75542
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75543
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75544

2、 Microsoft 产品安全漏洞

Microsoft 3D Viewer 是美国微软（Microsoft）公司的一款简化且快速的图形编辑应用程序。Microsoft 3D Builder 是微软公司的一款创建模型和 3D 打印的工具。Microsof

t Azure 是美国微软（Microsoft）公司的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，攻击者可利用漏洞获取域管理员权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft 3D Viewer 远程代码执行漏洞（CNVD-2023-74906、CNVD-2023-74905、CNVD-2023-74904）、Microsoft 3D Builder 远程代码执行漏洞（CNVD-2023-74907、CNVD-2023-74910、CNVD-2023-74909、CNVD-2023-74908）、Microsoft Azure HDInsight Apache Ambari 权限提升漏洞。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-2023-74906
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74905
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74904
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74907
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74910
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74909
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74908
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74911

3、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Thunderbird 是美国 Mozilla 基金会的一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。该软件支持 IMAP、POP 邮件协议以及 HTML 邮件格式。Mozilla Firefox ESR 是美国 Mozilla 基金会的 Firefox（Web 浏览器）的一个延长支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，使应用程序崩溃等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 内存错误引用漏洞（CNVD-2023-75343）、Mozilla Thunderbird 和 Firefox 拒绝服务漏洞、Mozilla Firefox ESR 代码问题漏洞（CNVD-2023-75346）、Mozilla Firefox 代码问题漏洞（CNVD-2023-75344）、Mozilla Firefox 整数溢出漏洞（CNVD-2023-75351）、Mozilla Firefox 远程代码执行漏洞、Mozilla Firefox 内存破坏漏洞（CNVD-2023-75349）、Mozilla Firefox 资源操作不当漏洞。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-2023-75343
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75347
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75346
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75344
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75351
https://www.cnvd.org.cn/flaw/show/CNVD-2023-75350

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75349

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75348

4、Siemens 产品安全漏洞

Siemens Parasolid 是一种三维几何建模工具，支持各种技术，包括实体建模、直接编辑和自由曲面/图纸建模。Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。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进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Parasolid 堆栈缓冲区溢出漏洞、Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2023-75582、CNVD-2023-75581、CNVD-2023-75583、CNVD-2023-75584）、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-75585、CNVD-2023-75586、CNVD-2023-75587）。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-2023-75579

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75582

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75581

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75583

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75585

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75584

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75586

https://www.cnvd.org.cn/flaw/show/CNVD-2023-75587

5、Open5GS 访问控制错误漏洞

Open5GS 是一个 5G Core 和 Epc 的 C 语言开源实现，即 Lte/Nr 网络的核心网络。本周，Open5GS 被披露存在访问控制错误漏洞。攻击者可利用该漏洞向 Open5GS 端点发送 HTTP 请求，并检索存储在设备上的信息。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-2023-76460

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-2023-74907	Microsoft 3D Builder 远程代码执行漏洞（CNVD-2023-74907）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-

			US/security-guidance/advisory/CVE-2023-36773
CNVD-2023-75350	Mozilla Firefox 远程代码执行漏洞	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.mozilla.org/en-US/security/advisories/mfsa2022-24/
CNVD-2023-75540	Google Android 权限提升漏洞（CNVD-2023-75540）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/2023-09-01
CNVD-2023-75574	Siemens Xpedition Layout Browser 堆栈溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-829656.html
CNVD-2023-75580	Siemens Tecnomatix Plant Simulation 文件分析漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-524778.html
CNVD-2023-75583	Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2023-75583）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-524778.html
CNVD-2023-75588	Siemens Simcenter Amesim 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-386812.html
CNVD-2023-75604	F5 BIG-IP 拒绝服务漏洞（CNVD-2023-75604）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K000137053
CNVD-2023-75609	F5 BIG-IP iControl 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K000137053
CNVD-2023-75606	F5 BIG-IP 拒绝服务漏洞（CNVD-2023-75606）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K000137053

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上运行任意代码。此外，Microsoft、Mozilla、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取域管理员权限，在当前进程的上下文中执行代码，使应用程序崩溃等。另外，Open5GS 被披露存在访问控制错误漏洞。攻击者可利用该漏洞向 Open5GS 端点发送 HTTP 请求，并检索存储在设备上的信息。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、TOTOLINK A3002R 缓冲区溢出漏洞

验证描述

TOTOLINK A3002R 是中国吉翁电子（TOTOLINK）公司的一款符合最新 IEEE802.11ac Wave 2 标准的无线双频千兆路由器。

TOTOLINK A3002R 存在缓冲区溢出漏洞，攻击者可利用该漏洞导致拒绝服务。

验证信息

POC 链接：https://github.com/1759134370/iot/blob/main/TOTOLINK/A3002R/3.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-76373

信息提供者

哈尔滨安天科技集团股份有限公司

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. 黑客正在利用 Citrix NetScaler 网关漏洞，收集用户凭证

Security Affairs 网站披露，IBM X-Force 研究人员发现威胁攻击者正在利用 Citrix NetScaler 网关存在的 CVE-2023-3519 漏洞（CVSS 评分：9.8），开展大规模的凭证收集活动。

参考链接：https://www.freebuf.com/news/380066.html

2. 以色列火箭警报应用程序 RedAlert 遭到黑客攻击

研究人员声称，亲巴勒斯坦黑客组织 AnonGhost 利用 RedAlert 应用程序中的缺陷发送了虚假的核攻击威胁。

参考链接：https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/

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