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 07 日-2023 年 08 月 13 日

2023 年第 32 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 473 个，其中高危漏洞 219 个、中危漏洞 238 个、低危漏洞 16 个。漏洞平均分值为 6.56。本周收录的漏洞中，涉及 0day 漏洞 367 个（占 78%），其中互联网上出现“Availability Booking Calendar PHP 跨站脚本漏洞、MotoCMS 代码执行漏洞”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 6410 个，与上周（28470 个）环比减少 77%。

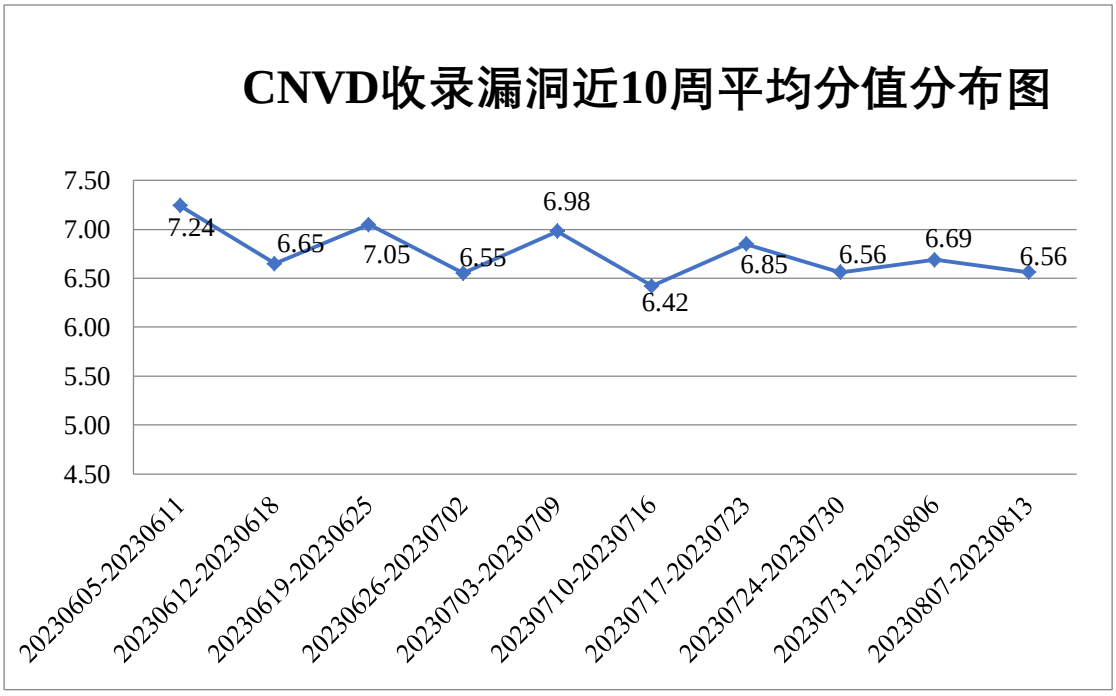

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 起，向基础电

信企业通报漏洞事件 10 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 789 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 98 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 35 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：

泰华智慧产业集团股份有限公司、金蝶软件（中国）有限公司、普联技术有限公司、深圳市米讯达信息技术有限公司、上海泛微网络科技股份有限公司、广州市溢信科技股份有限公司、吉翁电子（深圳）有限公司、北京星网锐捷网络技术有限公司、PbootCMS、北京新时空科技股份有限公司、上海海鼎信息工程股份有限公司、望海康信（北京）科技股份公司、广州图创计算机软件开发有限公司、江西铭软科技有限公司、深圳坐标软件集团有限公司、厦门市理臣教育服务有限公司、沧州市凡诺广告传媒有限公司、西安金讯通软件技术有限公司、杭州雄伟科技开发股份有限公司、北京易迅时代科技有限公司、奥琦玮信息科技（北京）有限公司、北京通达信科科技有限公司、北京百卓网络技术有限公司、友讯电子设备（上海）有限公司、山东大有医网医疗科技有限公司、长沙市同迅计算机科技有限公司、大连华天软件有限公司、南元泵业有限公司、北京万户软件技术有限公司、河南航天金穗电子有限公司、新希望物业服务集团有限公司、迈普通信技术股份有限公司、上海卓卓网络科技有限公司、北京亿赛通科技发展有限责任公司、申瓯通信设备有限公司、SEMCMS、广州优天网络科技有限公司、深圳典阅科技有限公司、上海斐讯数据通信技术有限公司、青岛灼灼文化传媒有限公司、广州恒企教育科技有限公司、天津神舟通用数据技术有限公司、深圳维盟科技股份有限公司、深圳市网心科技有限公司、杭州数栈科技有限公司、北京巧巧时代网络科技有限公司、深圳市必联电子有限公司、合肥贰道网络科技有限公司、深圳市博思协创网络科技有限公司、济南爱程网络科技有限公司、湖南壹拾捌号网络技术有限公司、摩莎科技（上海）有限公司、安徽生命港湾信息技术有限公司、安美世纪（北京）科技有限公司、北京人人检科技有限公司、北京天融信网络安全技术有限公司、北京致远互联软件股份有限公司、北京智慧远景科技产业有限公司、北京中创视讯科技有限公司、四川速帮时代科技有限公司、东方时尚驾驶学校股份有限公司、杭州海康威视数字技术股份有限公司、滴咚个游科技（广东）有限公司、恒生电子股份有限公司、弘扬软件股份有限公司、北京宏景世纪软件股份有限公司、江苏零浩网络科技有限公司、江西博微新技术有限公司、龙采科技集团有限责任公司、北方华创科技集团股份有限公司、杭州叙简科技股份有限公司、任子行网络技术股份有限公司、睿易教育科技股份有限公司、厦门四信通信科技有限公司、熵基科技股份有限公司、上海多维度网络科技股份有限公司、深圳致安视科技有限公司、神州通立电梯有限公司、武汉天地伟业科技有限公司、天津黑核科技有限公司、天津天堰科技股份有限公司、天闻数媒科技(北京)有限公司、深圳市威纶通科技有限公司、中

老文化艺术产业集团（海南）有限公司、武汉玖玖珈网络科技有限公司、一诺（鞍山）信息科技有限责任公司、中教畅享（北京）科技有限公司、珠海奔图打印科技有限公司、爱普生（中国）有限公司、用友网络科技股份有限公司、上海创旗天下科技股份有限公司、百富计算机技术（深圳）有限公司、湖南星云网络信息技术有限公司、深圳市倍泰健康测量分析技术有限公司、北京中教启星科技股份有限公司、深圳市吉祥腾达科技有限公司、东莞市一码网络科技有限公司、探探文化发展（北京）有限公司、深圳市蓝凌软件股份有限公司、Wavlink、北京西控电子商务有限公司、成都瑞安云科技股份有限公司、全天数据管理有限公司、北京勤云科技发展有限公司、三星（中国）投资有限公司、福建盟购信息科技有限公司、畅捷通信息技术股份有限公司、洛阳择兴实业有限公司、趋若信息科技有限公司、河南宅乐送生活科技有限公司、联奕科技股份有限公司、上海贝锐信息科技股份有限公司、城安盛邦（北京）网络科技股份有限公司、上海飞驴湾文化传播股份有限公司、淄博闪灵网络科技有限公司、上海阿法迪智能数字科技股份有限公司、正方软件股份有限公司、杭州爱讯科技有限公司、小明太极（湖北）国漫文化有限公司、北京用友政务软件股份有限公司、武汉达梦数据库有限公司、北京慕华信息科技有限公司、江苏金智科技股份有限公司、广州璐华信息技术有限公司、杭州吉拉科技有限公司、广东天波信息技术股份有限公司、常州文庭软件有限公司、青岛漫斯特数字科技有限公司、北京南琼电子有限责任公司、廊坊市极致网络科技有限公司、北京神州绿盟科技有限公司、浙江大华技术股份有限公司、深圳市领空技术有限公司、北京网康科技有限公司、上海肯特仪表股份有限公司、深圳市绿联科技股份有限公司、瑞斯康达科技发展股份有限公司、福州联讯信息科技有限公司、杭州奕锐电子有限公司、zzzcms、北京卓软在线信息技术有限公司、苍穹数码技术股份有限公司、北京五指互联科技有限公司、优慕课在线教育科技（北京）有限责任公司、杭州蓝代斯克数字技术有限公司、北京中远麒麟科技有限公司、垒知科技集团有限公司、华教教育科技（江西）有限公司和同程网络科技股份有限公司。

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、北京天融信网络安全技术有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、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。杭州美创科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、联想集团、安徽锋刃信息科技有限公司、河南信安世纪科技有限公司、重庆电信系统集成有限公司、成都安美勤信息技术股份有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、亚信科技（成都）有限公司、北京水木羽林科技有限公司、赛尔网络有限公司、浙江中控技术股份有限公司、陕西慧缘网络科技有限公司、河南省鼎信信息安全等级测评有限公司、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、中国烟草总公司湖北省公司、安徽思珀特信息科技有限公司、北京远禾科技有限公司、信息产业信息安全测评中心、河南悦海数安科技有限公司、任子行网络技术股份有限公司、北京云弈科技有限公司、河北锎远网络科技有限公司、江苏君立华域信息安全技术股份有限公司、深圳昂楷科技有限公司、安徽天行网安信息安全技术有限公司、北京东方通科技股份有限公司、南瑞集团公司（国网电力科学研究院）、浙江东安检测技术有限公司、西藏熙安信息技术有限责任公司、中华人民共和国广东海事局、深圳市魔方安全科技有限公司、中国银行、海南神州希望网络有限公司及其他个人白帽子向 CNVD 提交了 6410 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）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 4894 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）	3270	3270
斗象科技（漏洞盒子）	773	773
新华三技术有限公司	615	0
三六零数字安全科技集团有限公司	602	602
北京天融信网络安全技术有限公司	352	0
深信服科技股份有限公司	322	0
北京神州绿盟科技有限公司	262	0
上海交大	249	249
安天科技集团股份有限公司	160	0
阿里云计算有限公司	99	0
北京启明星辰信息安全技术有限公司	94	9
北京长亭科技有限公司	77	0
天津市国瑞数码安全系统股份有限公司	59	0
杭州迪普科技股份有	49	0

限公司		
北京知道创宇信息技术有限公司	36	3
杭州安恒信息技术股份有限公司	16	16
远江盛邦（北京）网络安全科技股份有限公司	16	16
南京众智维信息科技有限公司	7	7
浙江大华技术股份有限公司	2	2
北京智游网安科技有限公司	1	1
京东科技信息技术有限公司	1	1
杭州美创科技有限公司	207	207
奇安星城网络安全运营服务（长沙）有限公司	62	62
联想集团	36	36
西门子（中国）有限公司	35	0
安徽锋刃信息科技有限公司	35	35
河南信安世纪科技有限公司	23	23
重庆电信系统集成有限公司	18	18
成都安美勤信息技术股份有限公司	17	17
河南东方云盾信息技术有限公司	15	15
快页信息技术有限公	13	13

司		
亚信科技（成都）有限公司	11	11
北京水木羽林科技有限公司	10	10
赛尔网络有限公司	7	7
浙江中控技术股份有限公司	6	6
陕西慧缘网络科技有限公司	4	4
河南省鼎信信息安全等级测评有限公司	3	3
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	3	3
中国烟草总公司湖北省公司	3	3
安徽思珀特信息科技有限公司	3	3
北京远禾科技有限公司	2	2
信息产业信息安全测评中心	2	2
河南悦海数安科技有限公司	2	2
任子行网络技术股份有限公司	1	1
北京云弈科技有限公司	1	1
河北镌远网络科技有限公司	1	1
江苏君立华域信息安全技术股份有限公司	1	1
深圳昂楷科技有限公司	1	1

安徽天行网安信息安全技术有限公司	1	1
北京东方通科技股份有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
浙江东安检测技术有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
中华人民共和国广东海事局	1	1
深圳市魔方安全科技有限公司	1	1
中国银行	1	1
海南神州希望网络有限公司	1	1
CNCERT 广西分中心	4	4
CNCERT 贵州分中心	1	1
个人	960	960
报送总计	8558	6410

本周漏洞按类型和厂商统计

本周，CNVD 收录了 473 个漏洞。WEB 应用 214 个，应用程序 141 个，网络设备（交换机、路由器等网络端设备）70 个，操作系统 27 个，智能设备（物联网终端设备）14 个，安全产品 6 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	214
应用程序	141
网络设备（交换机、路由器等网络端设备）	70
操作系统	27
智能设备（物联网终端设备）	14
安全产品	6
车联网	1

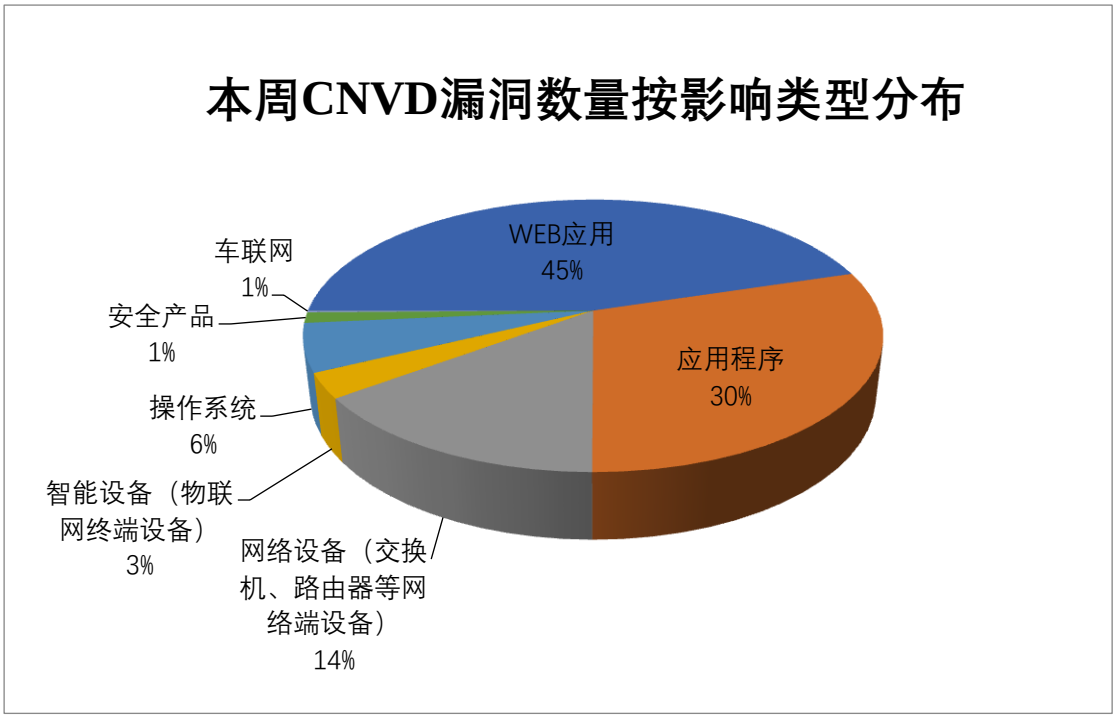

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、北京百卓网络技术有限公司、Huawei 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	31	7%
2	北京百卓网络技术有限公司	20	4%
3	Huawei	16	3%
4	Wireshark	11	2%
5	友讯电子设备（上海）有限公司	11	2%
6	JetBrains	10	2%
7	Mozilla	8	2%
8	Apple	8	2%
9	新华三技术有限公司	7	2%
10	其他	351	74%

本周行业漏洞收录情况

本周，CNVD 收录了 36 个电信行业漏洞，69 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，“Siemens RUGGEDCOM ROS 设备镜像端口隔离漏洞、

Rockwell Automation Kinetix 5700 拒绝服务漏洞”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/

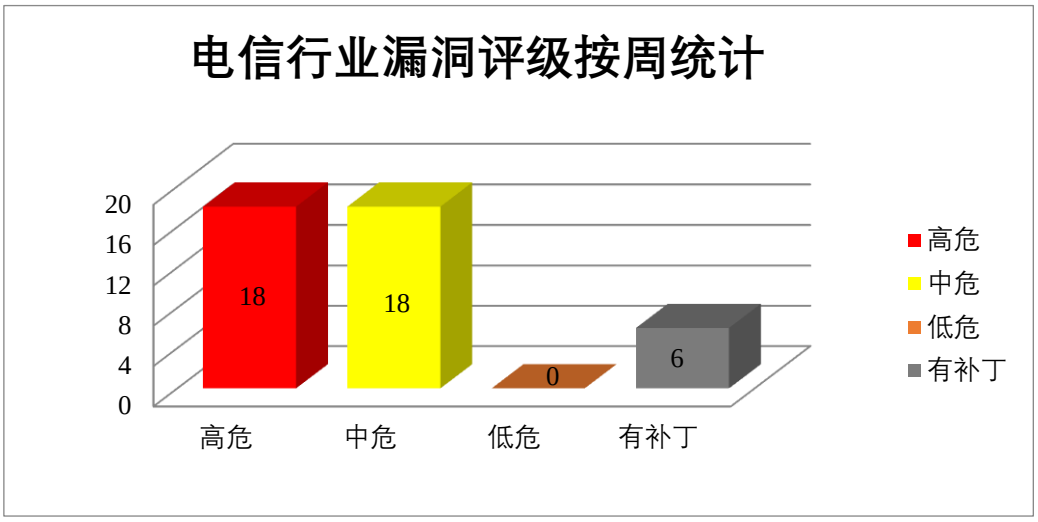

图 3 电信行业漏洞统计

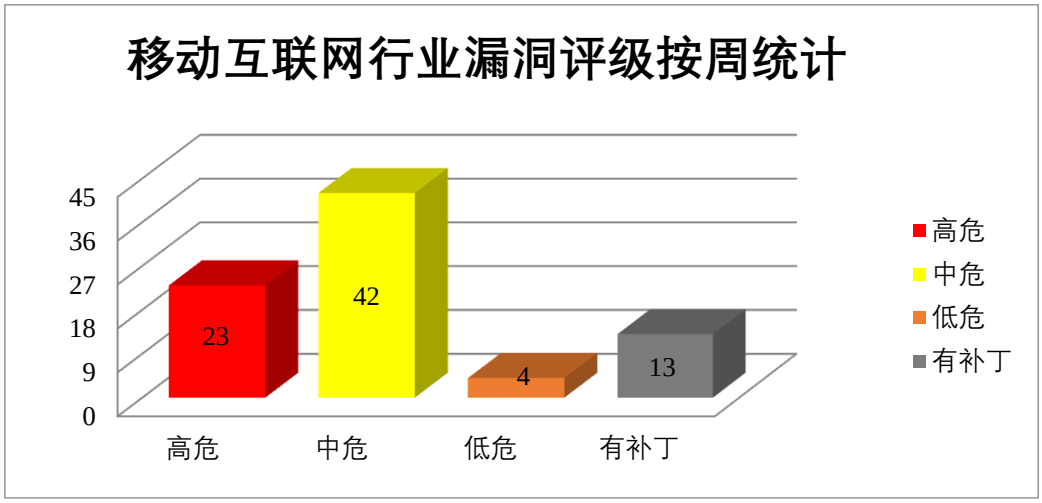

图 4 移动互联网行业漏洞统计

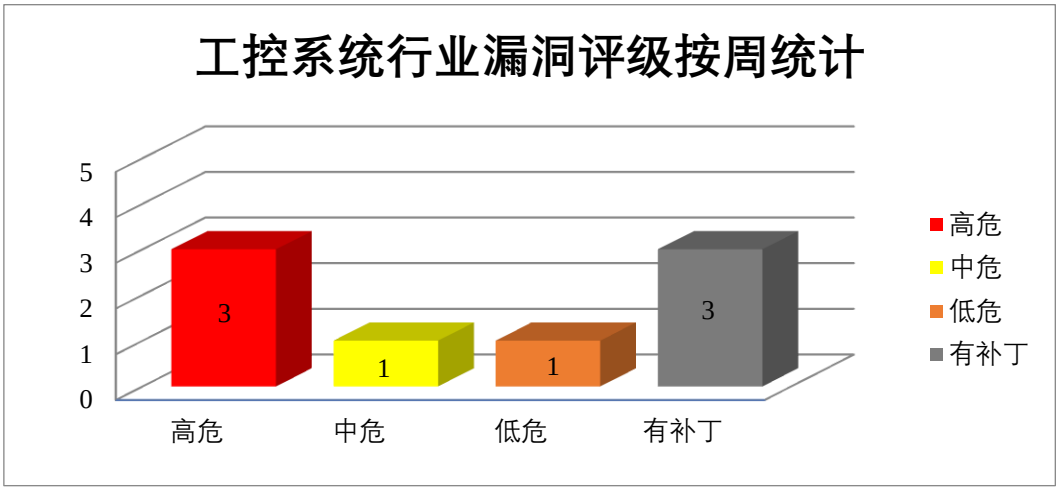

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei EMUI 是华为公司开发的一种基于 Android 操作系统的用户界面。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访问限制，获取敏感信息，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 和 EMUI 信息泄露漏洞（CNVD-2023-61716、CNVD-2023-61742、CNVD-2023-61743、CNVD-2023-61747）、Huawei HarmonyOS 和 EMUI 安全绕过漏洞（CNVD-2023-61717、CNVD-2023-61718）、Huawei HarmonyOS 和 EMUI 拒绝服务漏洞、Huawei HarmonyOS 信息泄露漏洞（CNVD-2023-61746）。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-2023-61716
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61717
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61718
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61742
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61743
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61745
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61746
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61747

2、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 Firefox ES

R 是火狐浏览器(企业版)。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限制，在易受攻击的系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox and Firefox ESR 安全绕过漏洞（CNVD-2023-61752、CNVD-2023-61751、CNVD-2023-61756、CNVD-2023-61755）、Mozilla Firefox and Firefox ESR 权限提升漏洞、Mozilla Firefox and Firefox ESR 拒绝服务漏洞（CNVD-2023-61753）、Mozilla Firefox 代码执行漏洞（CNVD-2023-61758）、Mozilla Firefox 欺骗漏洞（CNVD-2023-61757）。其中，除“Mozilla Firefox and Firefox ESR 安全绕过漏洞（CNVD-2023-61751、CNVD-2023-61756）、Mozilla Firefox and Firefox ESR 权限提升漏洞”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-2023-61752
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61751
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61756
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61755
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61754
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61753
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61758
https://www.cnvd.org.cn/flaw/show/CNVD-2023-61757

3、 Wireshark 产品安全漏洞

Wireshark 是一款具有流行度和影响力的开源协议分析器，常被用于网络故障排查、协议开发和教学等方面，其支持多种协议和数据格式。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，获取主机权限，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Wireshark 缓冲区溢出漏洞（CNVD-2023-62290、CNVD-2023-62287、CNVD-2023-62286、CNVD-2023-62289）、Wireshark 拒绝服务漏洞（CNVD-2023-62288、CNVD-2023-62294）、Wireshark 资源管理错误漏洞（CNVD-2023-62292）、Wireshark 无限循环漏洞（CNVD-2023-62291）。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-2023-62286
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62289
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62288
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62287
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62292
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62291

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62290

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62294

4、Siemens 产品安全漏洞

Solid Edge 是一个软件工具组合，可解决各种产品开发过程：3D 设计，仿真，制造和设计管理。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 Solid Edge 越界读取漏洞（CNVD-2023-62033、CNVD-2023-62032、CNVD-2023-62035、CNVD-2023-62034、CNVD-2023-62038、CNVD-2023-62037、CNVD-2023-62036）、Siemens Solid Edge 越界写入漏洞（CNVD-2023-62031）。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-2023-62033

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62032

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62031

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62035

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62034

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62038

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62037

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62036

5、ZKTeco BioAccess IVS 信息泄露漏洞

ZKTeco BioAccess IVS 是中国 ZKTeco 公司的一款基于 Web 的精简版安全平台。本周，ZKTeco BioAccess IVS 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取有关所有受管理设备的敏感信息。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-2023-62716

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-2023-61387	Foxit Reader 类型混淆漏洞（CNVD-2023-61387）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxitsoftware.cn/pdf-reader/?agent=foxit&MD=menu
CNVD-2023-61389	Foxit Reader 资源管理错误漏洞（CNVD-2023-61389）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxitsoftware.com/pdf-re

			ader/
CNVD-2023-61391	Rockwell Automation ThinManager 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140160
CNVD-2023-61741	Huawei HarmonyOS 和 EMUI 内存错误引用漏洞洞（CNVD-2023-61741）	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-202307-0000001587168858
CNVD-2023-61749	Huawei HarmonyOS 和 EMUI 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://device.harmonyos.com/cn/docs/security/update/security-bulletins-202307-0000001587168858
CNVD-2023-61750	Huawei HarmonyOS 和 EMUI 安全绕过漏洞（CNVD-2023-61750）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2023/7/
CNVD-2023-61765	Apple macOS Ventura 安全绕过漏洞（CNVD-2023-61765）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT213843
CNVD-2023-62040	Siemens RUGGEDCOM ROS 设备 Web 服务器拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-770902.html
CNVD-2023-62039	Siemens Solid Edge 越界写入漏洞（CNVD-2023-62039）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-811403.html
CNVD-2023-62046	Siemens Parasolid and Teamcenter Visualization 越界读取漏洞（CNVD-2023-62046）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-407785.html

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用漏洞绕过访问限制，获取敏感信息，造成拒绝服务等。此外，Mozilla、Wireshark、Siemens 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限制，在当前进程的上下文中执行代码，导致拒绝服务等。另外，ZKTeco BioAccess IVS 被披露存在信息泄露漏洞。攻击者可利用漏洞获取有关所有受管理设备的敏感信息。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、MotoCMS 代码执行漏洞

验证描述

MotoCMS 是 MotoCMS 公司的一个简单的网站构建器。

MotoCMS 存在代码执行漏洞，攻击者可利用该漏洞在系统上执行任意代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/51499

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-62829

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. Codesys V3 SDK 中的多个缺陷可能导致 RCE 或 DoS

Codesys 产品中的 16 个漏洞可能导致远程代码执行和 DoS 攻击，使 OT 环境暴露于黑客攻击之下。

参考链接：https://securityaffairs.com/149474/security/codesys-v3-sdk-rce-dos.html

2. Python URL 解析函数缺陷可以启用命令执行

Python URL 解析函数中的一个漏洞可以被利用来获得任意文件读取和命令执行。

参考链接：https://securityaffairs.com/149447/hacking/python-url-severe-vulnerability.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