

## 信息安全漏洞周报

2023年07月24日-2023年07月30日

2023年第30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 521 个，其中高危漏洞 272 个、中危漏洞 221 个、低危漏洞 28 个。漏洞平均分为 6.56。本周收录的漏洞中，涉及 0day 漏洞 456 个（占 88%），其中互联网上出现“ImpressCMS 跨站脚本漏洞（CNVD-2023-59104）、Food Ordering 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事件型漏洞总数 30305 个，与上周（8721 个）环比增多 2.47 倍。

### CNVD收录漏洞近10周平均分分布图

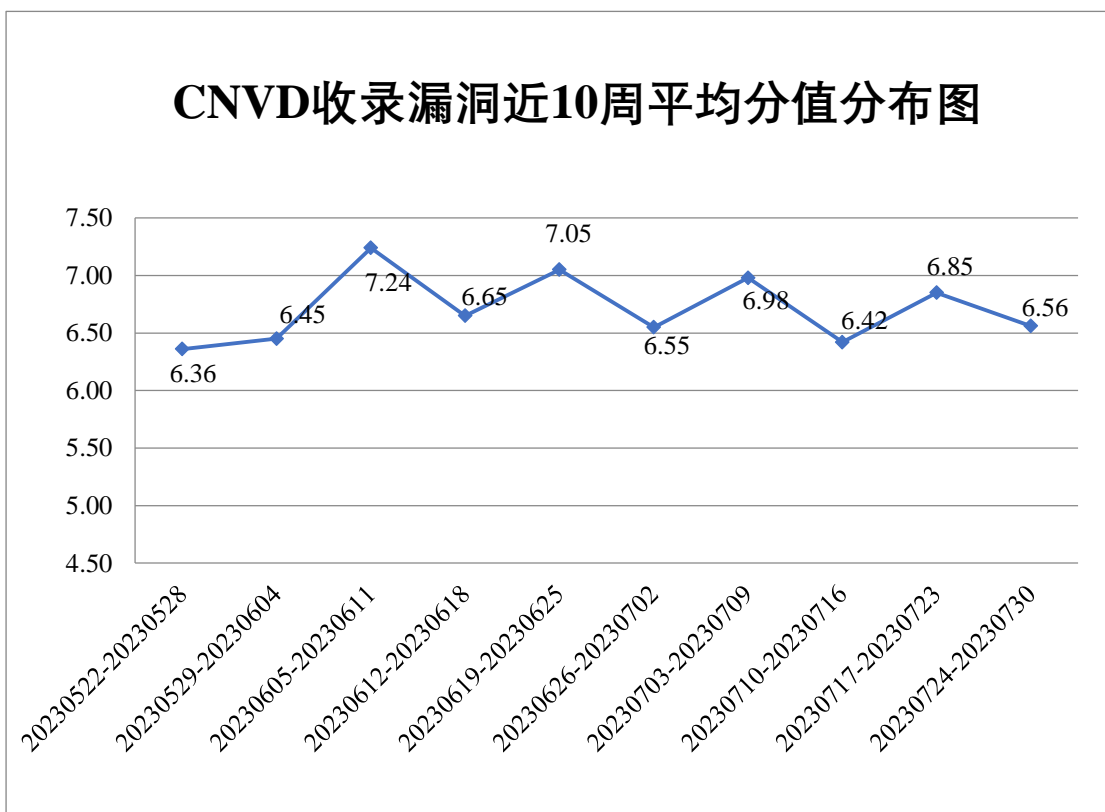



图 1 CNVD 收录漏洞近 10 周平均分分布图



## 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 23 起，向基础电信企业通报漏洞事件 5 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 672 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 124 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 56 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：

卓豪（中国）技术有限公司、珠海必要工业科技股份有限公司、中金亚洲（北京）国际互联网科技有限公司、中电鸿信信息科技有限公司、正方软件股份有限公司、浙江中控技术股份有限公司、浙江兰德纵横网络技术股份有限公司、浙江汇芸和实业集团有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、亚信科技（成都）有限公司、新开普电子股份有限公司、无锡信捷电气股份有限公司、温州互引信息技术有限公司、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、微特技术有限公司、威博通科技（上海）有限公司、望海康信（北京）科技股份公司、万达儿童文化发展有限公司、同程网络科技股份有限公司、天智（苏州）智能系统有限公司、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、天津搜鸽科技有限公司、遂成药业股份有限公司、苏州磐网通信技术有限公司、神州数码控股有限公司、深圳维盟网络技术有限公司、深圳市云屋科技有限公司、深圳市月歌科技有限公司、深圳市英威腾电气股份有限公司、深圳市思迅软件股份有限公司、深圳市普利华通讯设备有限公司、深圳市米进科技有限公司、深圳市蓝泰源信息技术股份有限公司、深圳市蓝凌软件股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市电速科技有限公司、深圳市迪洛斯电子科技有限公司、深圳市道尔智控科技股份有限公司、深圳市创互科技有限公司、深圳市博思协创网络科技有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海甄云信息科技有限公司、上海盈策信息技术有限公司、上海尚强信息科技有限公司、上海商汤智能科技有限公司、上海满孟信息科技有限公司、上海路团科技有限公司、上海居亦科技发展有限公司、上海九慧信息科技有限公司、上海华测导航技术股份有限公司、上海国际港务（集团）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、上海博达数据通信有限公司、上海安硕信息技术股份有限公司、熵基科技股份有限公司、山东中维世纪科技股份有限公司、山东运筹软件有限公司、山东捷瑞数字科技股份有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、任子行网络科技股份有限公司、桥西区雪洛软件开发工作室、麒麟软件有限公司、普联技术有限公司、南京云创大数据科技股份有限公司、南京医健通信息科技有限公司、秒联科技

(北京)有限公司、美了么信息科技有限公司、曼瑞德集团有限公司、迈普通信技术股份有限公司、联奕科技股份有限公司、联想集团、浪潮电子信息产业股份有限公司、景腾多媒体股份有限公司、江苏有线邦联新媒体科技有限公司、江苏曼荼罗软件股份有限公司、佳能(中国)有限公司、怀化南山田舍科技有限公司、合肥六出网络科技有限公司、杭州易软共创网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州网易竹邮科技有限公司、杭州飞致云信息科技有限公司、海星谷(大连)科技有限公司、海南赞赞网络科技有限公司、哈尔滨伟成科技有限公司、国泰新点软件股份有限公司、贵州飞利达科技股份有限公司、贵阳朗玛信息技术股份有限公司、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、广州鲁邦通物联网科技股份有限公司、广州华喜信息科技有限公司、广东振丰科教玩具有限公司、广东天琴信息技术有限公司、广东美胸汇网络科技有限公司、高新兴科技集团股份有限公司、福州富昌维控电子科技有限公司、佛山市淇特科技有限公司、东华医为科技有限公司、帝国软件、大连金马衡器有限公司、大汉软件股份有限公司、成都星锐蓝海网络科技有限公司、潮州市韩家网络科技有限公司、北京卓软在线信息技术有限公司、北京致远互联软件股份有限公司、北京医准智能科技有限公司、北京星网锐捷网络技术有限公司、北京心知堂文化交流有限公司、北京小鸟科技股份有限公司、北京五指互联科技有限公司、北京威速科技有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京商之讯软件有限公司、北京勤云科技发展有限公司、北京凝思软件股份有限公司、北京朗新天霁软件技术有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京海驾机动车驾驶员培训有限公司、北京国通创安报警网络技术有限公司、北京百卓网络技术有限公司、百度安全应急响应中心、安美世纪(北京)科技有限公司、安徽旭帆信息科技有限公司、安徽商信政通信息技术股份有限公司、Sapido Technology Inc、nginxWEBUI 和 NETGEAR。

## 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、北京启明星辰信息安全技术有限公司、安天科技集团股份有限公司、北京数字观星科技有限公司、新华三技术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、联想集团、安徽锋刃信息科技有限公司、重庆电信系统集成有限公司、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、杭州默安科技有限公司、赛尔网络有限公司、中国工商银行股份有限公司软件开发中心、博智安全科技股份有限公司、智网安云(武汉)信息技术有限公司、江苏君立华域信息安全技术股份有限公司、神州灵云(北京)科技有限公司、辽宁海事局、杭州弘沿科技有限公司、河南悦海数安科技有限公司、海南神州希望网络有限公司、上海蔚来汽车有限公司、深圳建安润星安全技术有限公司、宁夏

凯信特信息科技有限公司、亚信科技（成都）有限公司及其他个人白帽子向 CNVD 提交了 30305 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）、上海交大、奇安信网神（补天平台）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 29051 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）	22852	22852
斗象科技（漏洞盒子）	4246	4246
三六零数字安全科技集团有限公司	1029	1029
北京神州绿盟科技有限公司	958	2
上海交大	924	924
北京启明星辰信息安全技术有限公司	707	19
安天科技集团股份有限公司	313	0
北京数字观星科技有限公司	254	0
新华三技术有限公司	167	0
阿里云计算有限公司	99	0
北京天融信网络安全技术有限公司	70	10
天津市国瑞数码安全系统股份有限公司	38	0
北京长亭科技有限公司	29	0
杭州安恒信息技术股份有限公司	29	29
杭州迪普科技股份有限公司	20	0
北京知道创宇信息技术股份有限公司	4	0
卫士通信息产业股份	4	4

有限公司		
中国电信集团系统集成有限责任公司	2	2
杭州美创科技有限公司	126	126
联想集团	60	60
安徽锋刃信息科技有限公司	54	54
重庆电信系统集成有限公司	35	35
河南东方云盾信息技术有限公司	32	32
河南信安世纪科技有限公司	20	20
杭州默安科技有限公司	9	9
赛尔网络有限公司	6	6
中国工商银行股份有限公司软件开发中心	2	2
博智安全科技股份有限公司	2	2
智网安云（武汉）信息技术有限公司	1	1
江苏君立华域信息安全技术股份有限公司	1	1
神州灵云（北京）科技有限公司	1	1
辽宁海事局	1	1
杭州弘沿科技有限公司	1	1
河南悦海数安科技有限公司	1	1
海南神州希望网络科技有限公司	1	1
上海蔚来汽车有限公司	1	1

司		
深圳建安润星安全技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
亚信科技（成都）有限公司	1	1
CNCERT 广西分中心	7	7
CNCERT 宁夏分中心	2	2
CNCERT 浙江分中心	1	1
个人	821	821
报送总计	32933	30305

### 本周漏洞按类型和厂商统计

本周，CNVD 收录了 521 个漏洞。WEB 应用 362 个，网络设备（交换机、路由器等网络设备）67 个，应用程序 56 个，智能设备（物联网终端设备）11 个，操作系统 10 个，数据库 8 个，安全产品 7 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	362
网络设备（交换机、路由器等网络设备）	67
应用程序	56
智能设备（物联网终端设备）	11
操作系统	10
数据库	8
安全产品	7

## 本周CNVD漏洞数量按影响类型分布

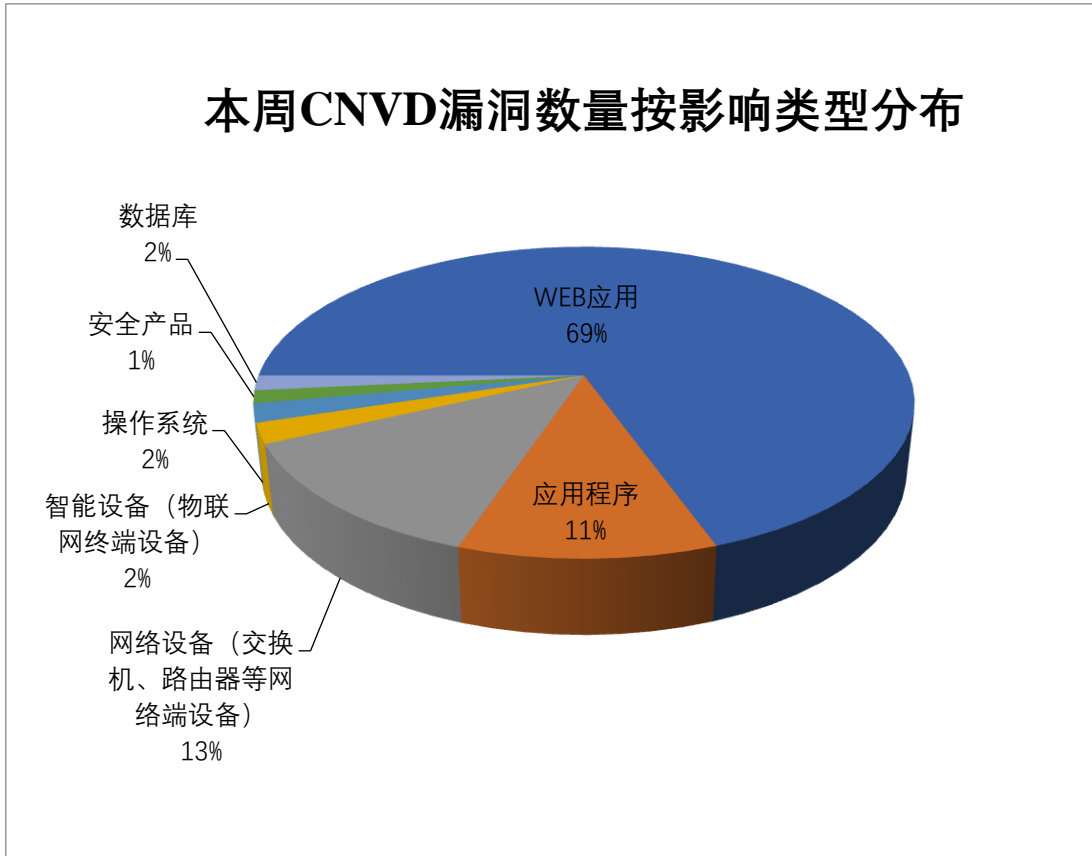


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京百卓网络技术有限公司、用友网络科技股份有限公司、IBM 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	北京百卓网络技术有限公司	19	4%
2	用友网络科技股份有限公司	16	3%
3	IBM	11	2%
4	Moxa	10	2%
5	Mozilla	9	2%
6	Linux	8	1%
7	北京宏景世纪软件股份有限公司	6	1%
8	北京星网锐捷网络技术有限公司	6	1%
9	北京网康科技有限公司	6	1%
10	其他	430	83%

本周，CNVD 收录了 44 个电信行业漏洞，25 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Tenda AC10 命令执行漏洞、Moxa SDS-3008 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/>

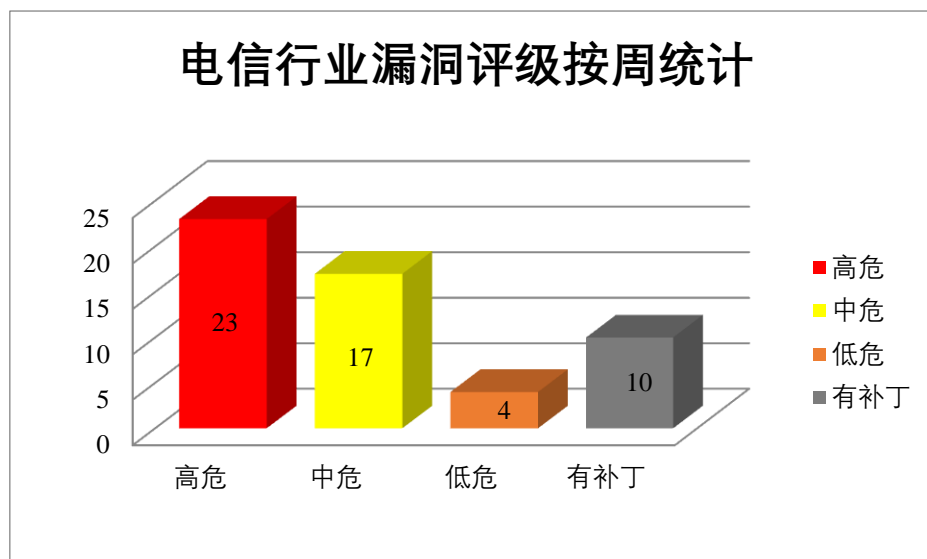


图 3 电信行业漏洞统计

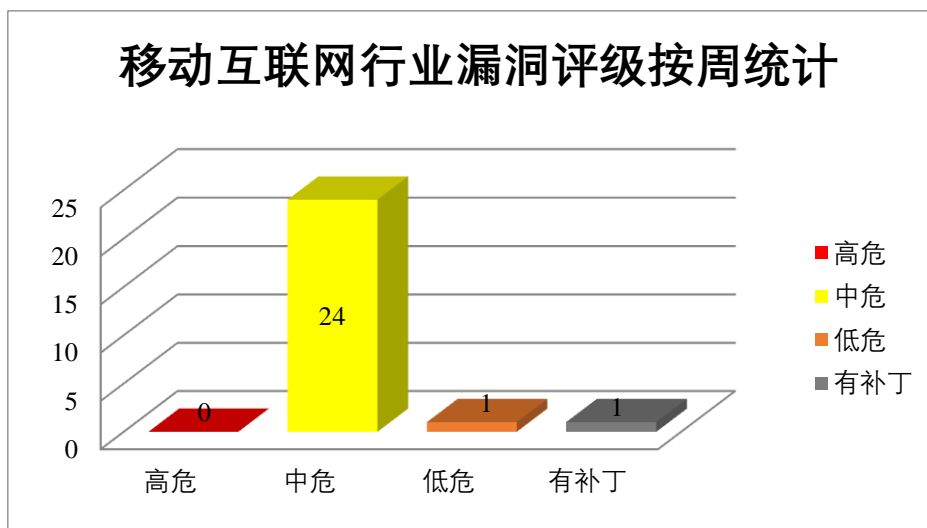


图 4 移动互联网行业漏洞统计



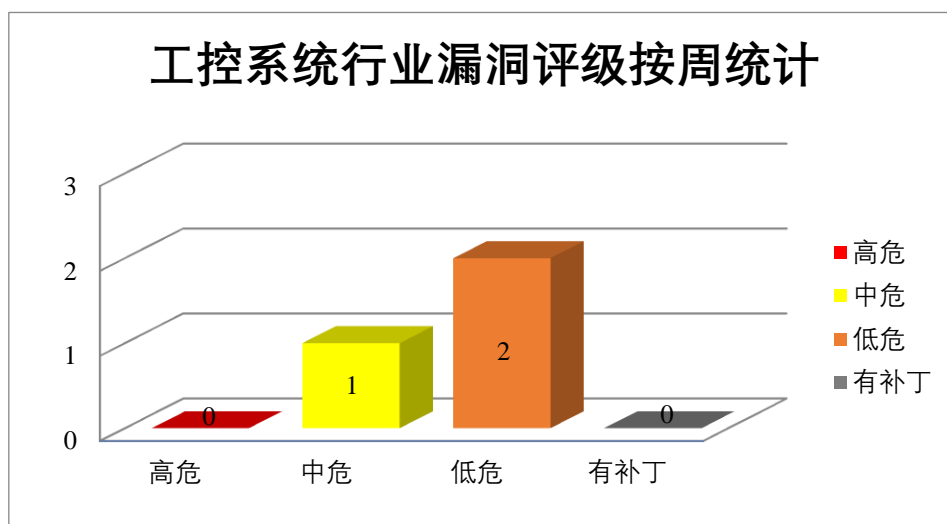


图 5 工控系统行业漏洞统计

## 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、IBM 产品安全漏洞

IBM AIX (Advanced Interactive eXecutive) 是美国 IBM 公司开发的一套 UNIX 操作系统。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，攻击者可利用漏洞执行任意命令，在受影响服务的路径中插入可执行文件来获得提升的权限等。

CNVD 收录的相关漏洞包括：IBM AIX 权限提升漏洞 (CNVD-2023-58513)、IBM AIX 命令执行漏洞、IBM DB2 代码执行漏洞 (CNVD-2023-58518、CNVD-2023-58517、CNVD-2023-58520)、IBM DB2 拒绝服务漏洞 (CNVD-2023-58519、CNVD-2023-58522)、IBM DB2 权限提升漏洞 (CNVD-2023-58521)。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-2023-58513>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58514>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58517>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58518>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58519>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58520>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58521>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58522>

## 2、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致内核信息泄露，将权限升级为 root 权限，在系统上执行任意代码或者导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Linux kernel 缓冲区溢出漏洞（CNVD-2023-58988、CNVD-2023-58993）、Linux kernel 资源管理错误漏洞（CNVD-2023-58987、CNVD-2023-58991、CNVD-2023-58989）、Linux kernel 竞争条件漏洞（CNVD-2023-58986）、Linux kernel xusb.c 文件代码问题漏洞、Linux kernel 输入验证错误漏洞（CNVD-2023-58992）。其中，“Linux kernel 缓冲区溢出漏洞（CNVD-2023-58993）”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-2023-58988>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58987>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58986>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58991>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58990>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58989>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58993>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58992>

## 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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过 HTTPS 创建 WebRTC 连接时触发释放后重用，提交特殊的 WEB 请求，诱使用户解析，可使系统崩溃，造成拒绝服务攻击或以应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 资源管理错误漏洞（CNVD-2023-58298、CNVD-2023-59025、CNVD-2023-59027、CNVD-2023-59029）、Mozilla Firefox 输入验证错误漏洞（CNVD-2023-59028）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-59026）、Mozilla Firefox 信息泄露漏洞（CNVD-2023-59031、CNVD-2023-59030）。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-2023-58298>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59025>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59028>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59027>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59026>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59031>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59030>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59029>

#### 4、Moxa 产品安全漏洞

Moxa MXsecurity 是中国摩莎（MOXA）公司的一个管理平台。可提供集中的可见性和安全管理，以轻松监视和识别网络威胁并防止安全错误配置，从而创建强大的威胁防御。Moxa SDS-3008 是中国摩莎（MOXA）公司的一系列工业交换机。Moxa NPort 5110 是 MOXA 的一款通用设备服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制 HTTP 请求导致任意 Javascript 执行，执行任意代码等。

CNVD 收录的相关漏洞包括：Moxa MXsecurity 命令注入漏洞、Moxa SDS-3008 跨站脚本漏洞（CNVD-2023-58304、CNVD-2023-58306、CNVD-2023-58305）、Moxa SDS-3008 明文传输漏洞、Moxa SDS-3008 拒绝服务漏洞、Moxa NPort 5110 越界写入漏洞、Moxa SDS-3008 信息泄露漏洞。其中，“Moxa MXsecurity 命令注入漏洞、Moxa SDS-3008 明文传输漏洞、Moxa SDS-3008 拒绝服务漏洞、Moxa NPort 5110 越界写入漏洞”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-2023-58300>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58304>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58303>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58302>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58308>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58307>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58306>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-58305>

#### 5、SEMCMS 代码问题漏洞

SEMCMS 是一套支持多种语言的外贸网站内容管理系统（CMS）。本周，SEMCMS 被披露存在代码问题漏洞。攻击者可利用该漏洞上传任意文件并获得升级的权限。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-2023-58823>

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-2023-58522	IBM DB2 拒绝服务漏洞(CNVD-2023-58522)	高	厂商已发布了漏洞修复程序，请及时关注更新：

			<a href="https://www.ibm.com/support/pages/node/7010557">https://www.ibm.com/support/pages/node/7010557</a>
CNVD-2023-58820	Advantech R-SeeNet 信任管理问题漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： <a href="https://icr.advantech.cz/products/software/r-seenet">https://icr.advantech.cz/products/software/r-seenet</a>
CNVD-2023-58819	FeehiCMS 任意文件上传漏洞 (CNVD-2023-58819)	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： <a href="https://github.com/liufee/cms/">https://github.com/liufee/cms/</a>
CNVD-2023-58822	IBM DB2 缓冲区溢出漏洞 (CNVD-2023-58822)	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.ibm.com/support/pages/node/7010565">https://www.ibm.com/support/pages/node/7010565</a>
CNVD-2023-58825	Piwigo SQL 注入漏洞 (CNVD-2023-58825)	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://github.com/Piwigo/Piwigo/security/advisories/GHSA-934w-qj9p-3qcx">https://github.com/Piwigo/Piwigo/security/advisories/GHSA-934w-qj9p-3qcx</a>
CNVD-2023-58824	SuiteCRM 跨站请求伪造漏洞 (CNVD-2023-58824)	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： <a href="https://huntr.dev/bounties/558b3dce-db03-47ba-b60b-c6eb578e04f1">https://huntr.dev/bounties/558b3dce-db03-47ba-b60b-c6eb578e04f1</a>
CNVD-2023-59032	Mozilla Thunderbird 缓冲区溢出漏洞 (CNVD-2023-59032)	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/">https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/</a>
CNVD-2023-59172	SpringBlade 安全模式绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://bladex.cn/">https://bladex.cn/</a>
CNVD-2023-58824	SuiteCRM 跨站请求伪造漏洞 (CNVD-2023-58824)	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://huntr.dev/bounties/558b3dce-db03-47ba-b60b-c6eb578e04f1">https://huntr.dev/bounties/558b3dce-db03-47ba-b60b-c6eb578e04f1</a>
CNVD-2023-58825	Piwigo SQL 注入漏洞 (CNVD-2023-58825)	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://github.com/Piwigo/Piwigo/security/advisories/GHSA-934w-qj9p-3qcx">https://github.com/Piwigo/Piwigo/security/advisories/GHSA-934w-qj9p-3qcx</a>

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意命令，在受影响服务的路径中插入可执行文件来获得提升的权限等。此外，Linux、Mozilla、Moxa 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致内核信息泄露，将权限升级为 root 权限，在系统上执行任意代码或者导致拒绝服务攻击等。另外，SEMCMMS 被披露

存在代码问题漏洞。攻击者可利用漏洞上传任意文件并获得升级的权限。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、ImpressCMS 跨站脚本漏洞（CNVD-2023-59104）

#### 验证描述

ImpressCMS 是一套基于 MySQL 的、模块化的内容管理系统（CMS）。该系统包括新闻发布、论坛和相册等模块。

ImpressCMS v1.4.5 及之前版本存在跨站脚本漏洞，该漏洞源于 editprofile.php 中的 smile\_code 参数对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

#### 验证信息

POC 链接：<https://github.com/CrownZTX/cve-description>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59104>

#### 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. MikroTik 操作系统漏洞暴露了 50 多万台设备

研究人员说，MikroTik RouterOS 漏洞使路由器受到特权升级攻击，允许威胁行为者完全控制易受攻击的设备。

参考链接：<https://cybernews.com/news/mikrotik-bug-exposes-thousands-devices/>

### 2. 新的人工智能工具“FraudGPT”出现，专为复杂攻击量身定制

跟随 WormGPT 的脚步，威胁行为者正在各种暗网市场和 Telegram 渠道上宣传另一种名为 FraudGPT 的网络犯罪生成人工智能（AI）工具。

参考链接：<https://thehackernews.com/2023/07/new-ai-tool-fraudgpt-emerges-tailored.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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82991537