国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 02 月 06 日-2023 年 02 月 12 日 **2023 年第 6 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 288 个，其中高危漏洞 126 个、中危漏洞 140 个、低危漏洞 22 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 182 个（占 63%），其中互联网上出现“drachtio-server 存在信息泄露漏洞、Hospital Management Center 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 5640 个，与上周（10419 个）环比减少 46%。

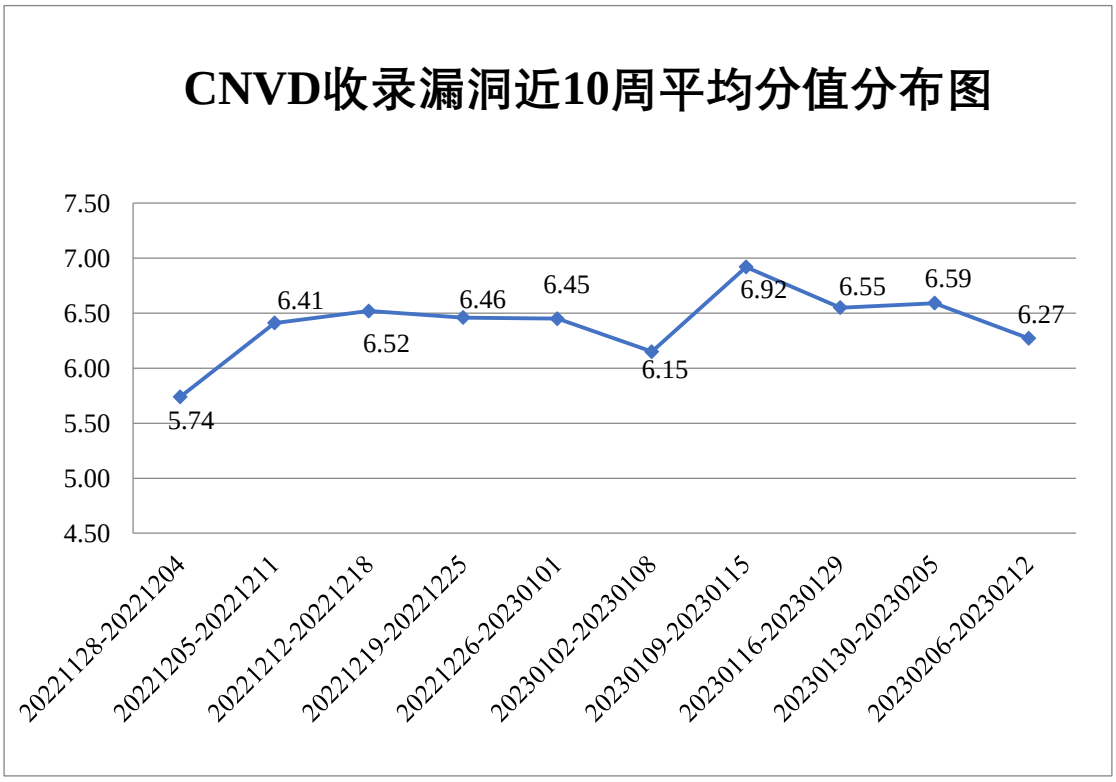

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 32 起，向基础电信企业通报漏洞事件 97 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 827 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 114 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 123 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：

卓想云创科技集团有限公司、珠海华发新科技投资控股有限公司、中音讯谷科技有限公司、中农国华农业科技（北京）有限公司、中科美络科技股份有限公司、智互联（深圳）科技有限公司、郑州天迈科技股份有限公司、浙江浙大中控信息技术有限公司、浙江花田网络有限公司、长沙中力大方信息技术有限公司、长沙市中智信息技术开发有限公司、长沙米拓信息技术有限公司、有品信息科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永辉超市股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、夏普科技（上海）有限公司、同望科技股份有限公司、四川众望升腾科技有限公司、施耐德电气（中国）有限公司、神州数码控股有限公司、深圳智慧光迅信息技术有限公司、深圳维盟科技股份有限公司、深圳拓安信物联股份有限公司、深圳市智国互联科技有限公司、深圳市思迅软件股份有限公司、深圳市深日科技有限公司、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、深圳市科荣软件股份有限公司、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、深圳市河辰通讯技术有限公司、深圳市广道数字技术股份有限公司、深圳科士达科技股份有限公司、深信服科技股份有限公司、上海卓卓网络科技有限公司、上海逐一软件科技有限公司、上海英立视数字科技有限公司、上海商汤智能科技有限公司、上海商派网络科技有限公司、上海软天文化传播有限公司、上海梦创双杨数据科技股份有限公司、上海建文软件科技有限公司、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、商派软件有限公司、山东欧倍尔软件科技有限责任公司、山东科德电子有限公司、山东港口科技集团日照有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、青果软件集团有限公司、千城智联（上海）网络科技有限公司、鹏为软件股份有限公司、迈普通信技术股份有限公司、康普科技(苏州)有限公司、敬业钢铁有限公司、江苏省广电有线信息网络股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、河北南昊高新技术开发有限公司、杭州三汇信息工程有限公司、杭州阔知网络科技有限公司、杭州荷花软件有限公司、杭州合泰软件有限公司、杭州飞致云信息科技有限公司、海南赞赞网络科技有限公司、广州易凯软件技术有限公司、广州芯德通信科技股份有限公司、广州网易计算机系统有限公司、福州联讯信息科技有限公司、烽火通信科技股份有限公司、得力集团有限公司、大庆紫金桥软件技

术有限公司、成都宏恒信息科技有限公司、成都飞鱼星科技股份有限公司、北京中成科信科技发展有限公司、北京用友政务软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京神州数码云科信息技术有限公司、北京派网软件有限公司、北京隆道网络科技有限公司、北京力控元通科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京华宇信息技术有限公司、北京宏景世纪软件股份有限公司、北京国炬信息技术有限公司、北京福田康明斯发动机有限公司、北京飞易腾科技有限公司、北京超图软件股份有限公司、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、保定飞凌嵌入式技术有限公司、傲拓科技股份有限公司和阿里巴巴集团安全应急响应中心。

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、深信服科技股份有限公司、安天科技集团股份有限公司、阿里云计算有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。上海齐同信息科技有限公司、北京升鑫网络科技有限公司、北京山石网科信息技术有限公司、苏州棱镜七彩信息科技有限公司、杭州默安科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、山东新潮信息技术有限公司、快页信息技术有限公司、杭州美创科技有限公司、内蒙古洞明科技有限公司、河南灵创电子科技有限公司、安徽锋刃信息科技有限公司、重庆易阅科技有限公司、博智安全科技股份有限公司、江苏金盾检测技术有限公司、北京安帝科技有限公司、重庆都会信息科技有限公司、西安敏恒信息技术有限公司、山东云天安全技术有限公司、广州安亿信软件科技有限公司、内蒙古中叶信息技术有限责任公司、平安银河实验室、赛尔网络有限公司、江苏保旺达软件技术有限公司、上海上讯信息技术股份有限公司、郑州埃文科技、墨菲未来科技（北京）有限公司、北京墨云科技有限公司、安徽安正测评技术有限公司、武汉提灯信息技术有限公司、云南联创网安科技有限公司、统信软件技术有限公司、宁夏凯信特信息科技有限公司、上海纽盾科技股份有限公司、北京惠而特科技有限公司、北京网御星云信息技术有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 5640 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）、上海交大和斗象科技（漏洞盒子）、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 3209 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
三六零数字安全科技集团有限公司	1404	1404
上海交大	984	984

新华三技术有限公司	639	0
斗象科技（漏洞盒子）	603	603
深信服科技股份有限公司	587	0
安天科技集团股份有限公司	270	0
阿里云计算有限公司	259	1
北京神州绿盟科技有限公司	243	1
奇安信网神（补天平台）	218	218
北京启明星辰信息安全技术有限公司	125	20
天津市国瑞数码安全系统股份有限公司	118	0
北京天融信网络安全技术有限公司	113	10
恒安嘉新（北京）科技股份公司	112	0
北京数字观星科技有限公司	98	0
卫士通信息产业股份有限公司	89	2
南京众智维信息科技有限公司	81	81
西安四叶草信息技术有限公司	69	69
中国电信集团系统集成有限责任公司	29	0
杭州安恒信息技术股份有限公司	19	0
杭州迪普科技股份有限公司	14	0
北京长亭科技有限公司	12	12

京东科技信息技术有限公司	8	0
北京信联数安科技有限公司	2	2
北京知道创宇信息技术有限公司	2	2
北京智游网安科技有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	1	1
北京华顺信安信息技术有限公司	109	0
上海齐同信息科技有限公司	91	91
北京升鑫网络科技有限公司	87	87
北京山石网科信息技术有限公司	47	47
苏州棱镜七彩信息科技有限公司	43	43
杭州默安科技有限公司	42	42
奇安星城网络安全运营服务（长沙）有限公司	35	35
河南东方云盾信息技术有限公司	32	32
山东新潮信息技术有限公司	29	29
快页信息技术有限公司	16	16
杭州美创科技有限公司	15	15
内蒙古洞明科技有限	14	14

公司		
河南灵创电子科技有限公司	11	11
安徽锋刃信息科技有限公司	9	9
重庆易阅科技有限公司	8	8
博智安全科技股份有限公司	8	8
江苏金盾检测技术有限公司	6	6
北京安帝科技有限公司	6	6
重庆都会信息科技有限公司	5	5
西安敏恒信息技术有限公司	5	5
山东云天安全技术有限公司	4	4
广州安亿信软件科技有限公司	4	4
内蒙古中叶信息技术有限责任公司	4	4
任子行网络技术股份有限公司	3	3
平安银河实验室	3	3
赛尔网络有限公司	3	3
江苏保旺达软件技术有限公司	3	3
上海上讯信息技术股份有限公司	2	2
郑州埃文科技	2	2
墨菲未来科技（北京）有限公司	1	1
北京墨云科技有限公	1	1

司		
安徽安正测评技术有限公司	1	1
武汉提灯信息技术有限公司	1	1
云南联创网安科技有限公司	1	1
统信软件技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
北京惠而特科技有限公司	1	1
北京网御星云信息技术有限公司	1	1
亚信科技（成都）有限公司	1	0
CNCERT 浙江分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 内蒙古分中心	1	1
CNCERT 广西分中心	1	1
个人	1676	1676
报送总计	8439	5640

本周漏洞按类型和厂商统计

本周，CNVD 收录了 288 个漏洞。WEB 应用 172 个，应用程序 72 个，网络设备（交换机、路由器等网络端设备）23 个，操作系统 12 个，智能设备（物联网终端设备）6 个，数据库 2 个，安全产品 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	172

应用程序	72
网络设备（交换机、路由器等网络端设备）	23
操作系统	12
智能设备（物联网终端设备）	6
数据库	2
安全产品	1

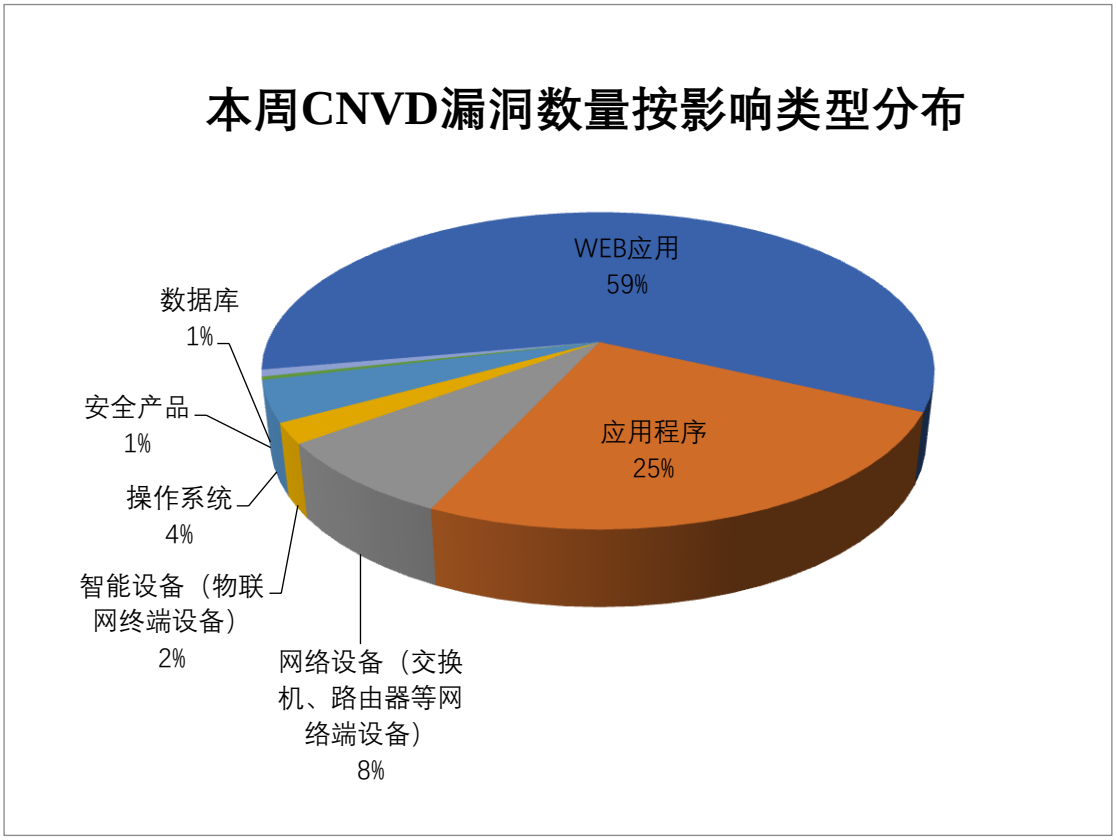

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Foxit、Google 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	WordPress	30	10%
2	Foxit	16	6%
3	Google	15	5%
4	Mozilla	11	4%
5	上海逐一软件科技有限公司	10	3%
6	Adobe	10	3%
7	ZKEACMS	8	3%
8	aerocms	7	3%

9	IBM	6	2%
10	其他	175	61%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，23 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2023-07647）、IBM WebSphere Application Server 代码注入漏洞”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/

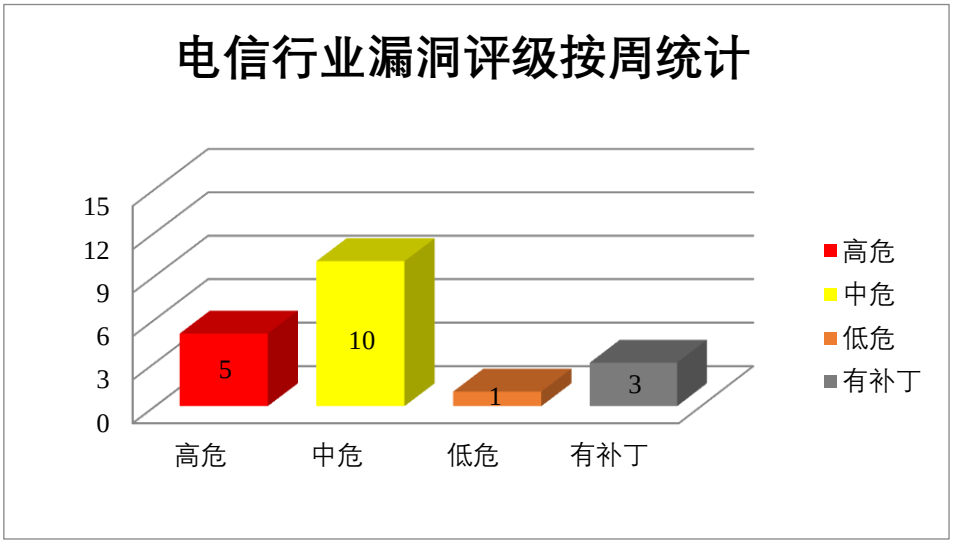

图 3 电信行业漏洞统计

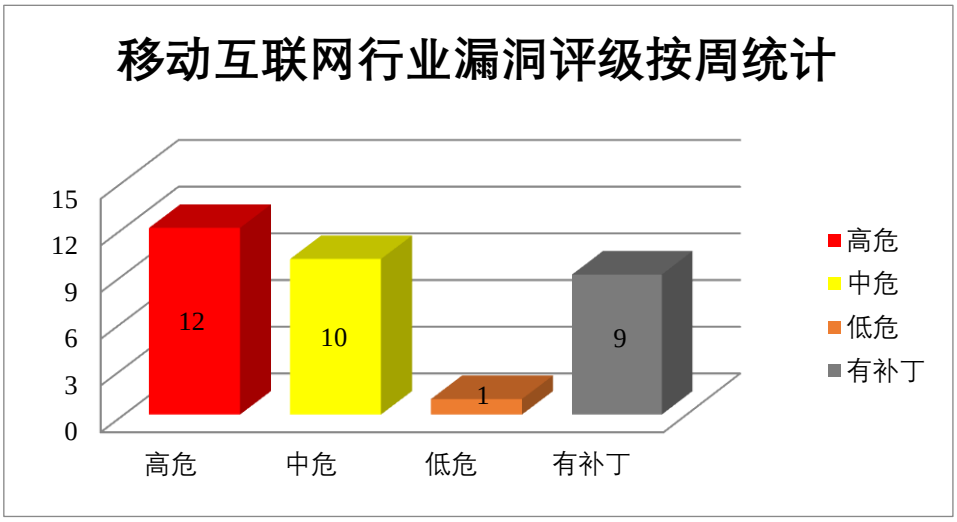

图 4 移动互联网行业漏洞统计

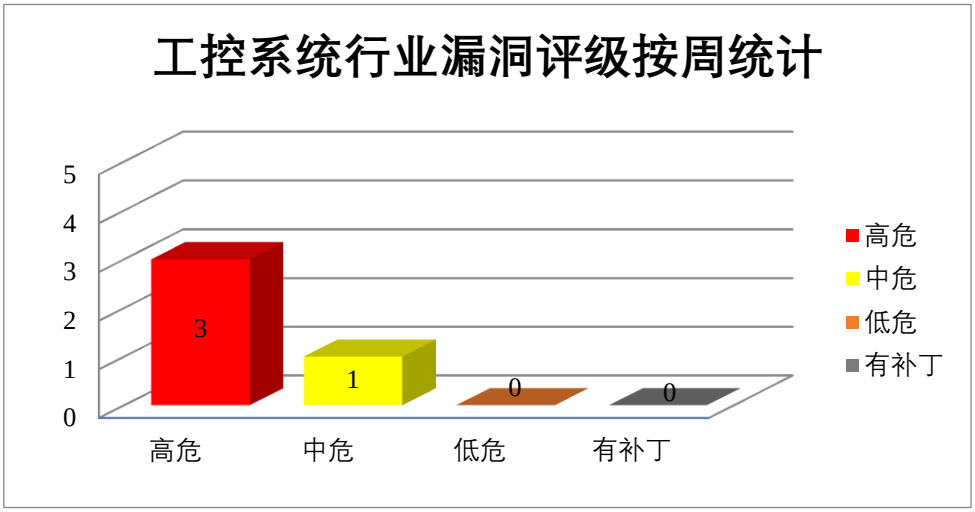

图 5 工控系统行业漏洞统计

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。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-07603、CNVD-2023-07604、CNVD-2023-07644、CNVD-2023-07646、CNVD-2023-07647）、Google Android 拒绝服务漏洞（CNVD-2023-07613）、Google Android 代码执行漏洞（CNVD-2023-07645）、Google Chrome Accessibility 代码执行漏洞。其中，除“Google Android 拒绝服务漏洞（CNVD-2023-07613）”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-2023-07603

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07604

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07613

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07644

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07645

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07646

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07647

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07703

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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发起跨站脚本攻击，绕过实施的安全限制，在目标系统上执行任意代码，导致程序崩溃等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-06858、CNVD-2023-06860、CNVD-2023-06865、CNVD-2023-06864）、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-06859）、Mozilla Firefox 输入验证错误漏洞（CNVD-2023-06861）、Mozilla Firefox 跨站脚本漏洞（CNVD-2023-06863）、Mozilla Firefox 安全特征问题漏洞（CNVD-2023-06862）。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-2023-06858
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06859
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06860
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06861
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06863
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06862
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06865
https://www.cnvd.org.cn/flaw/show/CNVD-2023-06864

3、 Adobe 产品安全漏洞

Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。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用户的上下文中任意执行代码，绕过 ASLR 等缓解措施，导致敏感内存泄露。

CNVD 收录的相关漏洞包括：Adobe Illustrator 越界读取漏洞（CNVD-2023-07320、CNVD-2023-07318、CNVD-2023-07317、CNVD-2023-07323、CNVD-2023-07322）、Adobe Illustrator 输入验证错误漏洞（CNVD-2023-07319、CNVD-2023-07321）、Adobe Illustrator 资源管理错误漏洞（CNVD-2023-07324）。其中“Adobe Illustrator 输入验证错误漏洞（CNVD-2023-07319、CNVD-2023-07321）、Adobe Illustrator 资源管理错误漏洞（CNVD-2023-07324）”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-2023-07320
https://www.cnvd.org.cn/flaw/show/CNVD-2023-07319
https://www.cnvd.org.cn/flaw/show/CNVD-2023-07318
https://www.cnvd.org.cn/flaw/show/CNVD-2023-07317
https://www.cnvd.org.cn/flaw/show/CNVD-2023-07323
https://www.cnvd.org.cn/flaw/show/CNVD-2023-07322

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07321

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07324

4、Foxit 产品安全漏洞

Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 阅读器。Foxit Reader 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。Foxit PDF Editor 是一款 PDF 编辑器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 内存错误引用漏洞（CNVD-2023-07826、CNVD-2023-07827、CNVD-2023-07828）、Foxit Reader 代码问题漏洞（CNVD-2023-07829）、Foxit PDF Reader 和 PDF Editor 代码问题漏洞、Foxit PDF Reader deletePages 远程代码执行漏洞、Foxit PDF Reader Doc 对象远程代码执行漏洞、Foxit PDF Reader Annotation 远程代码执行漏洞（CNVD-2023-07867）。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-2023-07826

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07827

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07828

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07829

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07843

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07865

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07866

https://www.cnvd.org.cn/flaw/show/CNVD-2023-07867

5、Tenda AC23 堆栈溢出漏洞

Tenda AC23 是中国腾达（Tenda）公司的一款双频千兆无线路由器。本周，Tenda AC23 被披露存在堆栈溢出漏洞，攻击者可利用该漏洞执行任意代码。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-2023-07906

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-2023-06535	WordPress plugin Master Elements 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://wpscan.com/vulnerability/a72bf075-fd4b-4aa5-b4a4-5f62a0620643

CNVD-2023-06866	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-06866）	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/mfsa2022-20/
CNVD-2023-07751	Google TensorFlow MirrorPadGrad 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gq2j-cr96-gvqx
CNVD-2023-07902	Foxit PDF Reader Annotation 远程代码执行漏洞（CNVD-2023-07902）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.foxit.com/support/security-bulletins.html
CNVD-2023-07759	LAVA 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.lavasoftware.org/archives/list/lava-announce@lists.lavasoftware.org/thread/WHXGQMIZAPW3GCQEXYHC32N2ZAAAIYCY
CNVD-2023-07757	Google TensorFlow tf.raw_ops.TensorListConcat 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-66vq-54fq-6jvv
CNVD-2023-07880	Foxit PDF Reader Annotation 远程代码执行漏洞（CNVD-2023-07880）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.foxit.com/support/security-bulletins.html
CNVD-2023-06857	Mozilla Firefox 资源管理错误漏洞（CNVD-2023-06857）	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/security/advisories/mfsa2021-52/
CNVD-2023-07758	Google TensorFlow tf.raw_ops.TensorListResize 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-67pf-62xr-q35m
CNVD-2023-07881	Foxit PDF Reader Doc 对象远程代码执行漏洞（CNVD-2023-07881）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.foxit.com/support/security-bulletins.html

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，在系统上执行任意代码，造成拒绝服务。此外，Mozilla、Adobe、Foxit 等多款产品被披露存

在多个漏洞，攻击者可利用漏洞发起跨站脚本攻击，绕过实施的安全限制，在目标系统上执行任意代码，导致拒绝服务等。另外，Tenda AC23 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞执行任意代码。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、drachtio-server 信息泄露漏洞

验证描述

drachtio-server 是 drachtio 开源的一个建立在 sofia SIP 堆栈上的 SIP 服务器。

drachtio drachtio-server 0.8.18 版本存在信息泄露漏洞，该漏洞源于本地用户可以检索敏感数据，攻击者可利用漏洞获取敏感信息。

验证信息

POC 链接：https://github.com/drachtio/drachtio-server/issues/241

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-07601

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. OpenSSL 通过最新更新修复了多个新的安全漏洞

OpenSSL 项目已发布修复程序以解决多个安全漏洞，包括开源加密工具包中的一个错误，该错误可能会使用户遭受恶意攻击。

参考链接：https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html

2. KeePass 曝安全漏洞，密码数据库被明文导出

近日，Bleeping Computer 网站披露，开源密码管理软件 KeePass 被爆存在安全漏洞 CVE-2023-24055，网络攻击者能够利用漏洞在用户毫不知情的情况下，以纯文本形式导出用户整个密码数据库。

参考链接：http://www.hackdig.com/02/hack-901895.htm

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