国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 12 月 18 日-2023 年 12 月 24 日 **2023 年第 51 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 563 个，其中高危漏洞 221 个、中危漏洞 283 个、低危漏洞 59 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 333 个（占 59%），其中互联网上出现“IceCMS 跨站脚本漏洞（CNVD-2023-98191）、LMXCMS SQL 注入漏洞（CNVD-2023-98192）”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 78107 个，与上周（45646 个）环比增加 71%。

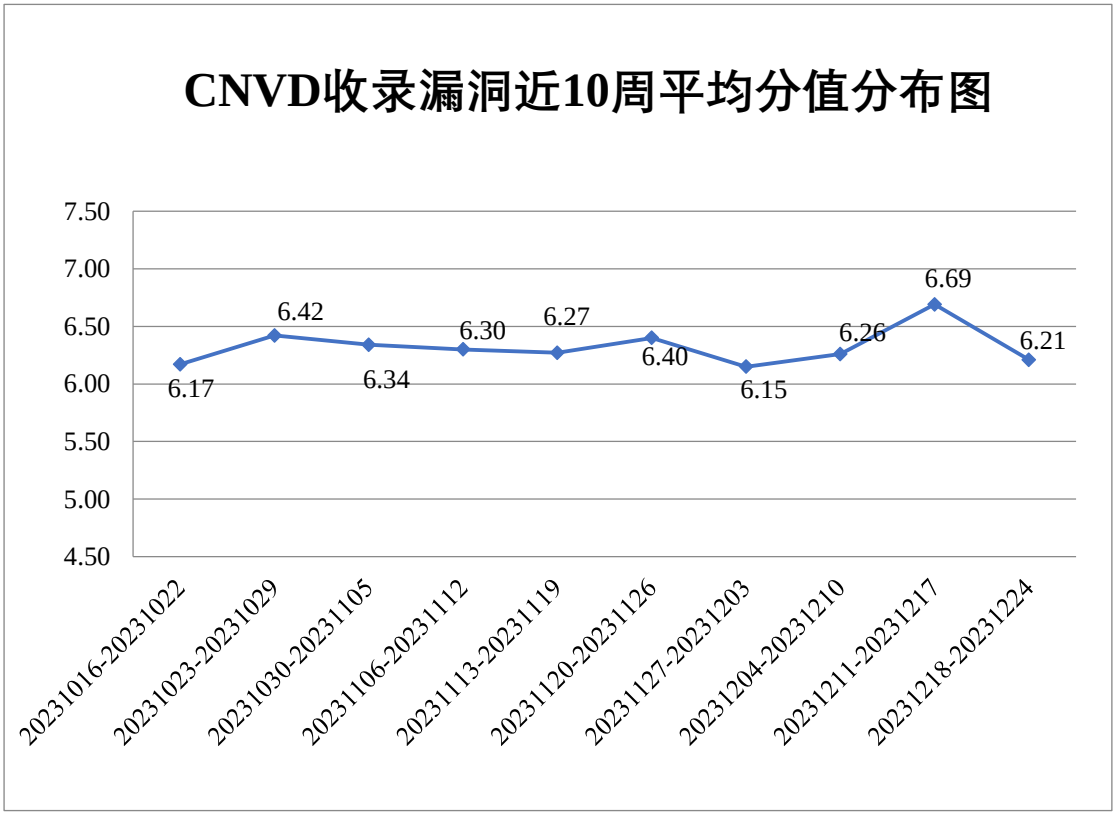

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 1175 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 214 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 33 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：

紫光软件系统有限公司、智享工场（深圳）科技有限公司、智石开工业软件有限公司、郑州蓝视科技有限公司、正奇晟业（北京）科技有限公司、浙江宇视科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、许继集团有限公司、信呼、新开普电子股份有限公司、武汉天际航信息科技股份有限公司、武汉达梦数据库股份有限公司、武汉北科天翼科技有限公司、网域数据安全（深圳）有限公司、网是科技股份有限公司、万洲电气股份有限公司、天闻数媒科技（北京）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、随锐科技集团股份有限公司、速达软件技术（广州）有限公司、苏州梦图地理信息系统有限责任公司、四川迅游网络科技股份有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市亿图软件有限公司、深圳市网心科技有限公司、深圳市明源云科技有限公司、深圳市美科星通信技术有限公司、深圳市领空技术有限公司、深圳市联新移动医疗科技有限公司、深圳市联天通信技术有限公司、深圳市联软科技股份有限公司、深圳市磊科实业有限公司、深圳市跨境伙伴网络科技有限公司、深圳市金蝶妙想互联有限公司、深圳市捷顺科技实业股份有限公司、深圳市顶讯网络科技有限公司、深圳市丛文安全电子有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海中云数赢云计算科技有限公司、上海云轴信息科技有限公司、上海英方软件股份有限公司、上海探链科技技术有限公司、上海软众网络科技有限公司、上海居亦科技发展有限公司、上海汇尼信息科技有限公司、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、上海安达通信息安全技术股份有限公司、山东云时空信息科技有限公司、山东潍微科技股份有限公司、山东科德电子有限公司、山东比特智能科技股份有限公司、厦门科拓通讯技术股份有限公司、厦门才茂通信科技有限公司、欧姆龙自动化（中国）有限公司、绵阳探云科技有限公司、美林数据技术股份有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、联想（北京）有限公司、蓝网科技股份有限公司、江苏中越科技发展有限公司、江苏麦维智能科技有限公司、江苏金智科技股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南壹拾捌号网络技术有限公司、湖南迪文科技有限公司、红星到家（上海）科技有限公司、合肥六出网络科技有限公司、杭州

雄伟科技开发股份有限公司、杭州瑞利声电技术有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、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、广州市玄武无线科技股份有限公司、广西耀象文化传播有限责任公司、广联达科技股份有限公司、广东保伦电子股份有限公司、富士施乐（中国）有限公司、阜阳市众诚软件有限公司、福建科立讯通信有限公司、福建九天达信息科技股份有限公司、福建博思软件股份有限公司、佛山市杜特软件科技有限公司、帝国软件、大庆紫金桥软件技术有限公司、成都行行行科技有限公司、成都生动网络科技有限公司、成都软视科技有限公司、成都华栖云科技有限公司、畅捷通信息技术股份有限公司、博彦科技股份有限公司、贝呗付科技开发有限公司、北京卓软在线信息技术有限公司、北京用友政务软件股份有限公司、北京英克康健科技有限公司、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、北京信安世纪科技有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京天行网安信息技术有限责任公司、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、北京数科网维技术有限责任公司、北京市地铁运营有限公司、北京润乾信息系统技术有限公司、北京派网软件有限公司、北京朗新天霁软件技术有限公司、北京金山办公软件股份有限公司、北京慧图科技（集团）股份有限公司、北京翰博尔信息技术股份有限公司、北京超粮科技有限责任公司、北京北信源软件股份有限公司、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、安翼物联网（南京）有限公司、安徽旭帆信息科技有限公司、安徽生命港湾信息技术有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心和 seacms。

本周，CNVD 发布了《关于蓝牙协议存在中间人攻击漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9576

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、深信服科技股份有限公司、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。中孚安全技术有限公司、快页信息技术有限公司、江苏金盾检测技术股份有限公司、贵州多彩网安科技有限公司、北京山石网科信息技术有限公司、河南灵创电子科技有限公司、河南东方云盾信息技术有限公司、内蒙古洞明科技有限公司、南京聚铭网络科技有限公司、亚信科技（成都）有限公司、安徽锋刃信息科技有限公司、浙江安腾信息技术有限公司、江苏晟晖信息科技有限公司、北京中睿天下信息技术有限公司、信息产业信息安全测评中心、西藏熙安信息技术有限责任公司、广州安亿信软件科技有限公司、江苏百达智慧网络科技有限公

司、星云博创科技有限公司、北京远禾科技有限公司、成方金融科技有限公司上海分公司、北京天防安全科技有限公司、河南悦海数安科技有限公司、深圳昂楷科技有限公司、北京卓识网安技术股份有限公司、联想集团、北京源堡科技有限公司、四川奇安旌服科技有限公司、成都安美勤信息技术股份有限公司、北京星网锐捷网络技术有限公司、信联科技（南京）有限公司、上海观安信息技术股份有限公司、赛尔网络有限公司、海南神州希望网络有限公司、杭州弘沿科技有限公司、南京共美科技有限公司、杭州智顺科技有限公司、北京科技大学、南京深安科技有限公司、国网湖北省电力有限公司恩施供电公司及其他个人白帽子向 CNVD 提交了 78107 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）、奇安信网神（补天平台）、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 76290 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）	46700	46700
奇安信网神（补天平台）	28810	28810
上海交大	397	397
北京天融信网络安全技术有限公司	5981	5
天津市国瑞数码安全系统股份有限公司	830	0
新华三技术有限公司	726	0
深信服科技股份有限公司	397	0
三六零数字安全科技集团有限公司	383	383
北京神州绿盟科技有限公司	377	0
北京数字观星科技有限公司	336	0
阿里云计算有限公司	316	2
安天科技集团股份有限公司	299	0
北京知道创宇信息技术有限公司	100	0
京东科技信息技术有	92	0

限公司		
北京启明星辰信息安全技术有限公司	85	0
北京长亭科技有限公司	56	3
北京安信天行科技有限公司	19	19
杭州迪普科技股份有限公司	10	0
中电科网络安全科技股份有限公司	9	9
南京联成科技发展股份有限公司	5	5
西安四叶草信息技术有限公司	2	2
北京智游网安科技有限公司	1	1
中孚安全技术有限公司	126	126
快页信息技术有限公司	120	120
江苏金盾检测技术股份有限公司	71	71
贵州多彩网安科技有限公司	65	65
北京山石网科信息技术有限公司	57	57
河南灵创电子科技有限公司	56	56
河南东方云盾信息技术有限公司	36	36
内蒙古洞明科技有限公司	32	32
南京聚铭网络科技有限公司	19	19

亚信科技（成都）有限公司	18	18
安徽锋刃信息科技有限公司	16	16
浙江安腾信息技术有限公司	14	14
江苏晟晖信息科技有限公司	10	10
北京中睿天下信息技术有限公司	6	6
信息产业信息安全测评中心	4	4
西藏熙安信息技术有限责任公司	3	3
广州安亿信软件科技有限公司	3	3
江苏百达智慧网络科技有限公司	3	3
星云博创科技有限公司	3	3
北京远禾科技有限公司	2	2
成方金融科技有限公司上海分公司	2	2
北京天防安全科技有限公司	2	2
河南悦海数安科技有限公司	2	2
深圳昂楷科技有限公司	2	2
北京卓识网安技术股份有限公司	2	2
联想集团	2	2
北京源堡科技有限公司	1	1

四川奇安旌服科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
北京星网锐捷网络技术有限公司	1	1
信联科技（南京）有限公司	1	1
上海观安信息技术股份有限公司	1	1
赛尔网络有限公司	1	1
海南神州希望网络有限公司	1	1
杭州弘沿科技有限公司	1	1
南京共美科技有限公司	1	1
杭州智顺科技有限公司	1	1
北京科技大学	1	1
南京深安科技有限公司	1	1
国网湖北省电力有限公司恩施供电公司	1	1
CNCERT 宁夏分中心	5	5
CNCERT 贵州分中心	5	5
个人	1071	1071
报送总计	87702	78107

本周漏洞按类型和厂商统计

本周，CNVD 收录了 563 个漏洞。WEB 应用 254 个，应用程序 157 个，网络设备（交换机、路由器等网络端设备）75 个，操作系统 41 个，智能设备（物联网终端设备）15 个，数据库 13 个，安全产品 8 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	254
应用程序	157
网络设备（交换机、路由器等网络端设备）	75
操作系统	41
智能设备（物联网终端设备）	15
数据库	13
安全产品	8

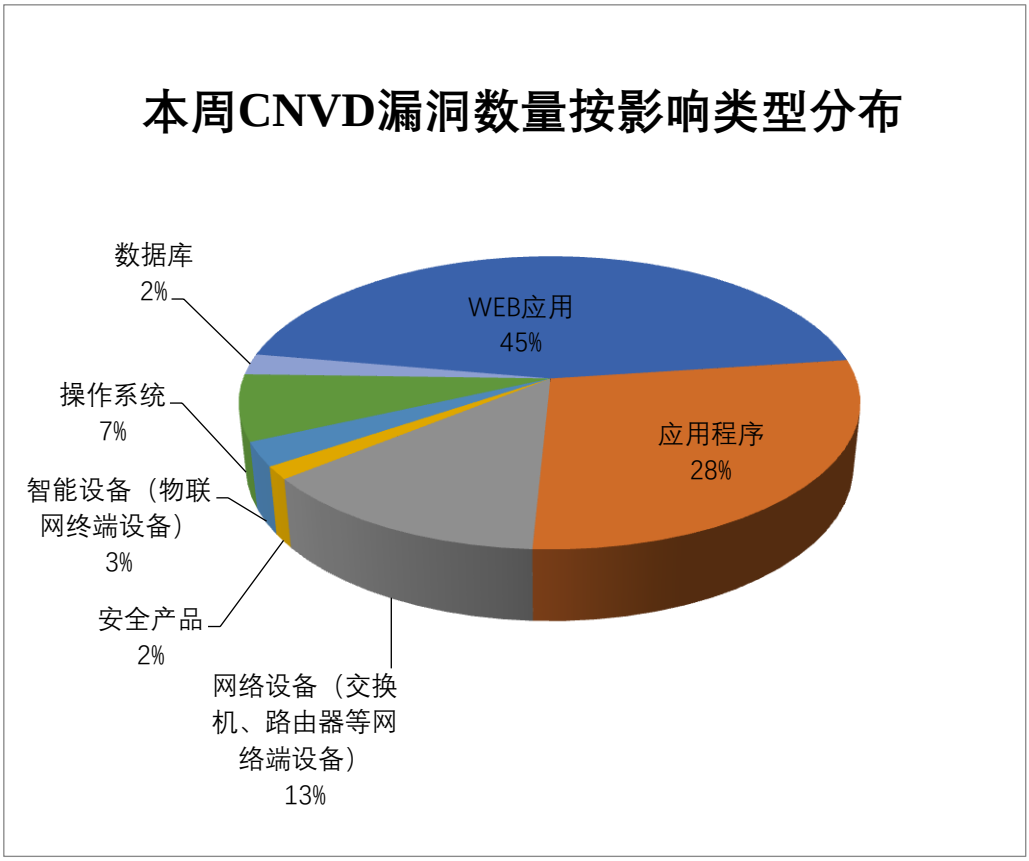

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、WordPress、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	Adobe	39	7%
2	WordPress	38	7%
3	Google	23	4%
4	Samsung	15	3%
5	吉翁电子（深圳）有限公司	13	2%

6	Tenda	13	2%
7	北京百卓网络技术有限公司	13	2%
8	Fortinet	11	2%
9	北京星网锐捷网络技术有限公司	8	2%
10	其他	390	69%

本周行业漏洞收录情况

本周，CNVD 收录了 57 个电信行业漏洞，58 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“ZTE MC801A 命令注入漏洞、TOTOLINK X6000R 访问控制错误漏洞”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/

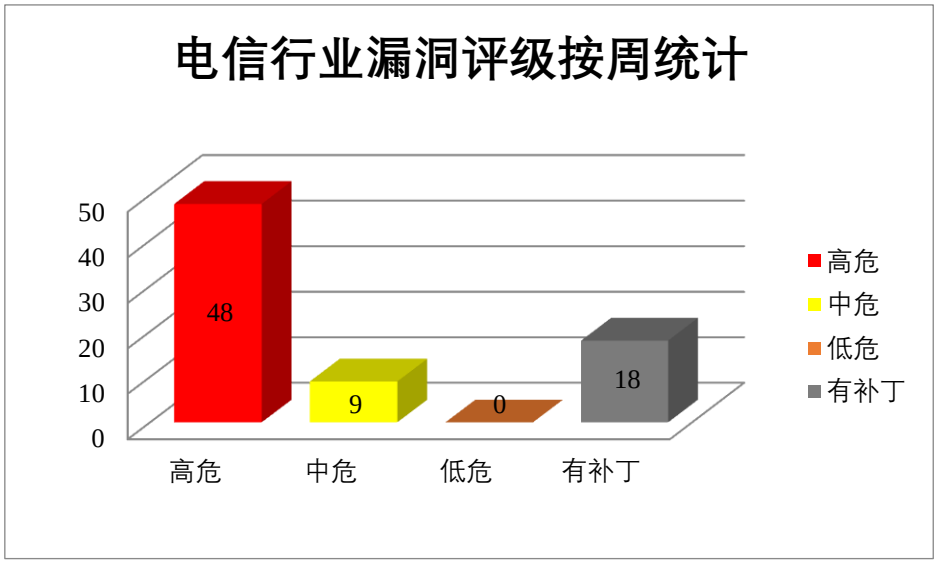

图 3 电信行业漏洞统计

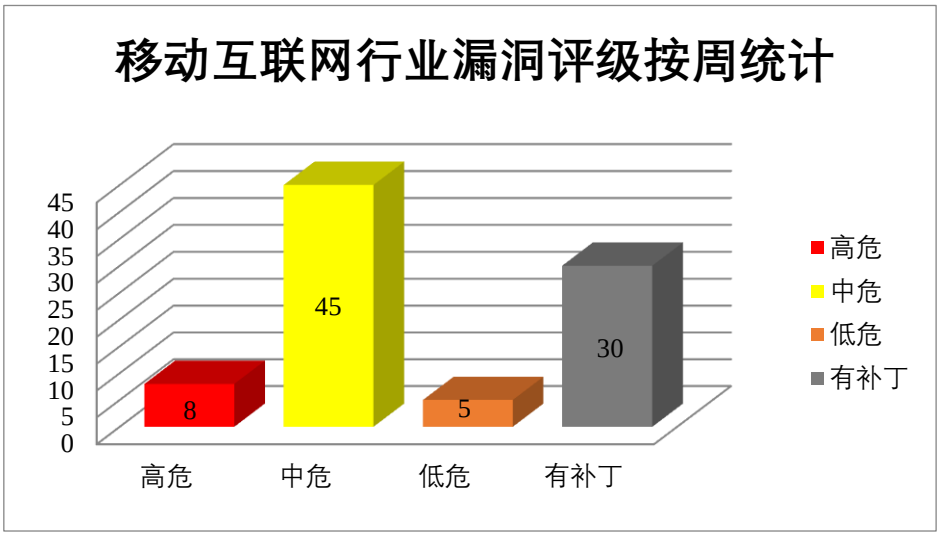

图 4 移动互联网行业漏洞统计

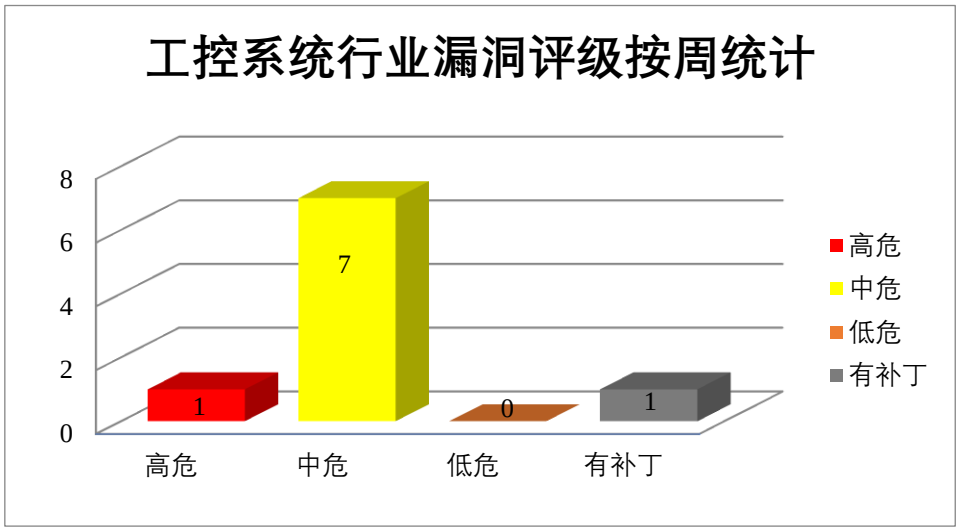

图 5 工控系统行业漏洞统计

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 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。IBM Planning Analytics 是美国国际商业机器（IBM）公司的一套业务规划分析解决方案。该方案支持自动化执行业务规划、预算和分析等流程。IBM Sterling B2B Integrator 是美国国际商业机器（IBM）公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。IBM Content Navigator 是美国国际商业机器（IBM）公司的一款 Web 客户机。该产品支持从 Web 浏览器搜索和处理存储在内容服务器中的文档。本周，上述产品被披露存在多个漏洞，攻击者可

利用漏洞获取敏感信息，造成 DoS，在 Web UI 中嵌入任意 JavaScript 代码，从而导致受信任会话中的凭据泄露等。

CNVD 收录的相关漏洞包括：IBM Db2 输入验证错误漏洞（CNVD-2023-98172、CNVD-2023-98171、CNVD-2023-98170、CNVD-2023-98174、CNVD-2023-98173）、IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2023-98177）、IBM Content Navigator 跨站脚本漏洞（CNVD-2023-98176）、IBM Planning Analytics 信息泄露漏洞（CNVD-2023-9817594）。其中“IBM Db2 输入验证错误漏洞（CNVD-2023-9817184、CNVD-2023-9817085、CNVD-2023-9817341）”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-2023-98172
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98171
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98170
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98175
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98174
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98173
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98177
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98176

2、 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，攻击者可利用漏洞获得提升的权限，导致拒绝服务，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-98746、CNVD-2023-98745、CNVD-2023-98748、CNVD-2023-98747）、Google Android 拒绝服务漏洞（CNVD-2023-98749、CNVD-2023-98754、CNVD-2023-98756）、Google Android 代码执行漏洞（CNVD-2023-98757）。其中，除“Google Android 拒绝服务漏洞（CNVD-2023-98749）”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-2023-98746
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98745
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98748
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98747
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98749
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98754

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98756

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98757

3、 Adobe 产品安全漏洞

Adobe RoboHelp 是美国奥多比（Adobe）公司的针对 Windows 开发和发布的帮助创作工具。Adobe Substance 3D Sampler 是美国奥多比（Adobe）公司的一款摄影测量软件。用于将照片捕捉和扫描图像转换为 3D 纹理和材质资产。Adobe Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。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敏感内存泄露，执行非法 SQL 命令窃取数据库敏感数据，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe RoboHelp SQL 注入漏洞、Adobe Substance 3D Sampler 越界写入漏洞（CNVD-2023-98212、CNVD-2023-98211、CNVD-2023-98215、CNVD-2023-98214、CNVD-2023-98213、CNVD-2023-98216）、Adobe Dimension 越界读取漏洞（CNVD-2023-9821791）。其中，除“Adobe Dimension 越界读取漏洞（CNVD-2023-9821791）”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-2023-98206

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98212

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98211

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98215

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98214

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98213

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98216

https://www.cnvd.org.cn/flaw/show/CNVD-2023-98217

4、 Fortinet 产品安全漏洞

Fortinet FortiClient 是美国飞塔（Fortinet）公司的一套移动终端安全解决方案。该方案与 FortiGate 防火墙设备连接时可提供 IPsec 和 SSL 加密、广域网优化、终端合规和双因子认证等功能。Fortinet FortiADC 是美国飞塔（Fortinet）公司的一款应用交付控制器。Fortinet FortiSIEM 是美国飞塔（Fortinet）公司的一套安全信息和事件管理系统。该系统包括资产发现、工作流程自动化和统一管理等功能。Fortinet FortiMail 是美国飞塔（Fortinet）公司的一套电子邮件安全网关产品。该产品提供电子邮件安全防护和数据保护等功能。Fortinet FortiEDR 是美国飞塔（Fortinet）公司的一个从头开始构建的端点安全解决方案。Fortinet FortiWLM 是美国飞塔（Fortinet）公司的一个无线管理器。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搜索路径中的恶意 OpenSSL 引擎库执行 DLL 劫持攻击，通过结构自动化 CLI 脚本的特定精心设计的配置将其权

限升级为 super_admin，通过特制的 CLI 请求执行任意代码或命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiClient 路径遍历漏洞（CNVD-2023-98182）、Fortinet FortiADC 访问控制错误漏洞、Fortinet FortiADC 缓冲区溢出漏洞、Fortinet FortiSIEM 信息泄露漏洞（CNVD-2023-98186）、Fortinet FortiMail 身份验证错误漏洞、Fortinet FortiEDR 访问控制错误漏洞（CNVD-2023-98184、CNVD-2023-98187）、Fortinet FortiSIEM 命令执行漏洞（CNVD-2023-98190）。其中，“Fortinet FortiADC 访问控制错误漏洞、Fortinet FortiMail 身份验证错误漏洞、Fortinet FortiSIEM 命令执行漏洞（CNVD-2023-98190）、Fortinet FortiEDR 访问控制错误漏洞”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-2023-98182
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98181
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98180
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98186
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98185
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98184
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98190
https://www.cnvd.org.cn/flaw/show/CNVD-2023-98187

5、D-Link DIR-846 反序列化漏洞

D-Link DIR-846 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-846 被披露存在反序列化漏洞。攻击者可利用该漏洞导致代码执行。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-2023-98193

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-2023-98179	Huawei HarmonyOS DFR 模块授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2023/12/
CNVD-2023-98205	Linux kernel 越界读取漏洞（CNVD-2023-98205）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.spinics.net/lists/stable-commits/msg303065.html
CNVD-2023	Tenda AC10 compare_parent	高	厂商已发布了漏洞修复程序，请及

-98204	control_time 函数缓冲区溢出漏洞		时关注更新：https://www.tenda.com.cn/
CNVD-2023-98209	Huawei HarmonyOS 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2023/10/
CNVD-2023-98208	Huawei HarmonyOS 拒绝服务漏洞（CNVD-2023-98208）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2023/10/
CNVD-2023-98741	libexpat 缓冲区错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/libexpat/libexpat/pull/550
CNVD-2023-98759	SharpZipLib 任意文件写入漏洞（CNVD-2023-98759）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/icsharpcode/SharpZipLib/commit/a0e96de70b5264f4c919b09253b1522bc7a221cc
CNVD-2023-98763	Apple macOS ColorSync 缓冲区错误漏洞	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/HT213054
CNVD-2023-98767	WordPress Essential Addons for Elementor plugin 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://wpscan.com/vulnerability/0d02b222-e672-4ac0-a1d4-d34e1ecf4a95
CNVD-2023-99030	Asterisk 缓冲区溢出漏洞（CNVD-2023-99030）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/asterisk/asterisk/security/advisories/GHSA-98rc-4j27-74hh

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，造成 DoS，在 Web UI 中嵌入任意 JavaScript 代码，从而导致受信任会话中的凭据泄露等。此外，Google、Adobe、Fortinet 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获得提升的权限，导致拒绝服务，在系统上执行任意代码，通过搜索路径中的恶意 OpenSSL 引擎库执行 DLL 劫持攻击，通过结构自动化 CLI 脚本的特定精心设计的配置将其权限升级为 super_admin，通过特制的 CLI 请求执行任意代码或命令等。另外，D-Link DIR-846 被披露存在反序列化漏洞。攻击者可利用漏洞导致代码执行。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、IceCMS 跨站脚本漏洞（CNVD-2023-98191）

验证描述

IceCMS 是一个基于 Spring Boot + Vue 前后端分离的内容管理系统。

IceCMS 2.0.1 版本存在跨站脚本漏洞。该漏洞源于应用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：http://39.106.130.187/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-98191

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. Android 恶意软件 Chameleon 禁用指纹解锁以窃取 PIN

Chameleon Android 银行木马以新版本重新出现，该版本使用一种棘手的技术来接管设备——禁用指纹和面部解锁来窃取设备 PIN。

参考链接：https://www.bleepingcomputer.com/news/security/android-malware-chameleon-disables-fingerprint-unlock-to-steal-pins/

2. 伊朗黑客利用 FalseFont 向全球国防工业基地发起攻击

近日，微软称伊朗网络间谍组织 APT33 正在利用 FalseFont 后门恶意软件攻击全球国防工业基地。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-hackers-target-defense-firms-with-new-falsefont-malware/

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