国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 11 月 21 日-2022 年 11 月 27 日 **2022 年第 47 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 536 个，其中高危漏洞 193 个、中危漏洞 261 个、低危漏洞 82 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 344 个（占 64%），其中互联网上出现“Microfinance Management System SQL 注入漏洞、Radare2 缓冲区溢出漏洞（CNVD-2022-81355）”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 39112 个，与上周（17037 个）环比增加 1.3 倍。

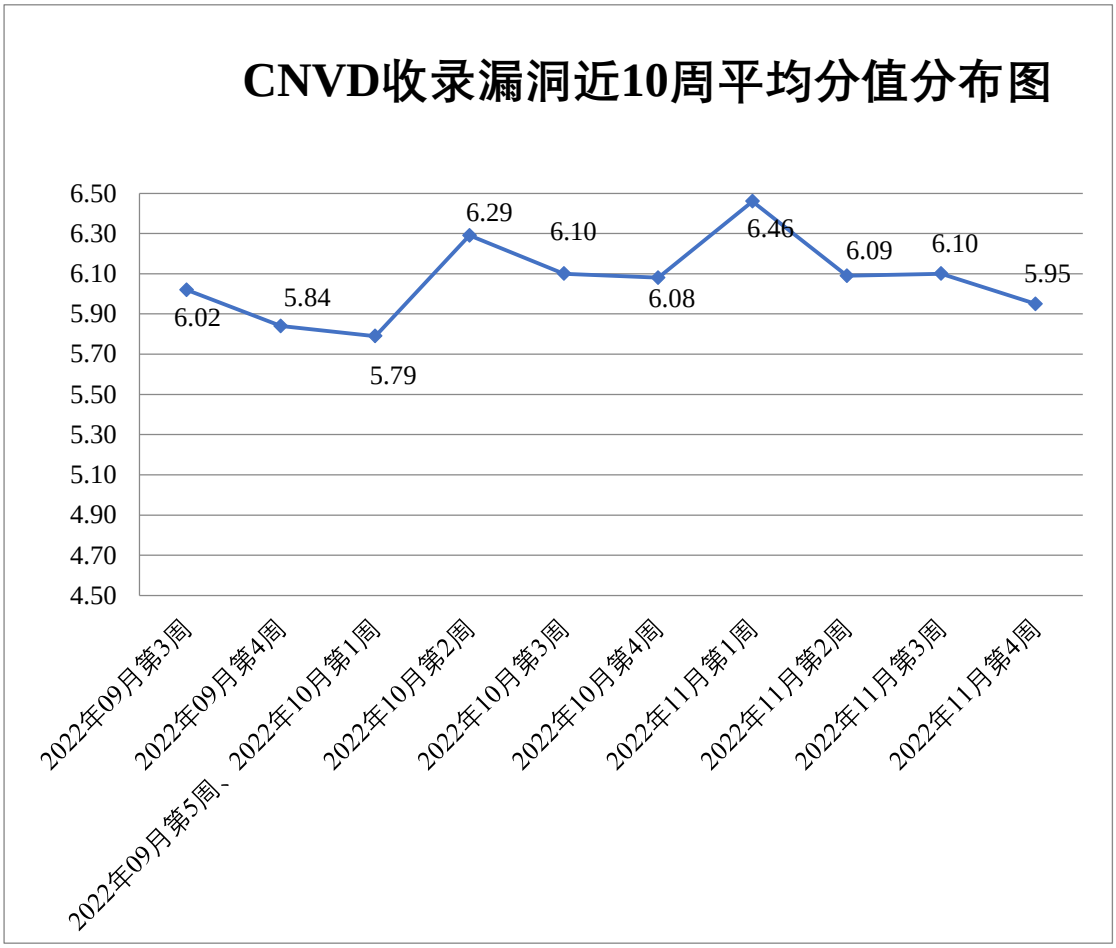

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 41 起，向基础电信企业通报漏洞事件 26 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 1097 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 210 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 174 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：

珠海国津软件科技有限公司、重庆紫光华山智安科技有限公司、重庆啄木鸟网络科技有限公司、重庆中联信息产业有限责任公司、重庆远秋科技股份有限公司、重庆玖玖洪海科技有限公司、重庆金算盘软件有限公司、重庆泛普软件有限公司、中农国华农业科技（北京）有限公司、中联重科股份有限公司、中电科新型智慧城市研究院有限公司、智互联（深圳）科技有限公司、智恒科技股份有限公司、浙江大华技术股份有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新浪网技术（中国）有限公司、携程旅行网、校无忧科技网络公司、夏普科技（上海）有限公司、武汉网幂科技有限公司、武汉思维跳跃科技有限公司、无锡享同信息科技有限公司、伟乐视讯科技股份有限公司、微脉技术有限公司、天津同阳科技发展有限公司、天津天创数字科技有限公司、台达集团、苏州伟创电气科技股份有限公司、苏州科达科技股份有限公司、深圳小鹅网络技术有限公司、深圳维盟科技股份有限公司、深圳市西迪特科技股份有限公司、深圳市万网博通科技有限公司、深圳市天视通技术有限公司、深圳市探鸽智能科技有限公司、深圳市乔安科技有限公司、深圳市农博创新科技有限公司、深圳市龙信信息技术有限公司、深圳市联软科技股份有限公司、深圳市金蝶天燕云计算股份有限公司、深圳市吉祥腾达科技有限公司、深圳市华远智能设备有限公司、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、深圳康柚健康科技有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海商汤智能科技有限公司、上海陌远网络科技有限公司、上海脉信网络科技有限公司、上海金榜智能科技有限公司、上海技腾通讯设备有限公司、上海汇尼信息科技有限公司、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、上海道裕物流科技有限公司、上海大众出行信息技术股份有限公司、上海博达数据通信有限公司、山西万鸿科技有限公司、山东博硕自动化技术有限公司、厦门市民数据服务股份有限公司、厦门神州鹰软件科技有限公司、三碁电气集团、青岛雨诺网络信息股份有限公司、奇偶科技股份（上海）有限公司、普联技术有限公司、鹏为软件股份有限公司、南京云网汇联软件技术有限公司、南京远古软件有限公司、南昌

航天广信科技有限责任公司、美团安全应急响应中心、浪潮通用软件有限公司、廊坊市极致网络科技有限公司、金蝶天燕云计算股份有限公司、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、吉奥时空信息技术股份有限公司、惠普贸易（上海）有限公司、华为技术有限公司、湖南瀚屯科技有限公司、河南上洋信息科技有限公司、河南斧牛网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、杭州爱惠信息技术有限公司、海尔集团、贵州觅新科技有限公司、广州图创计算机软件开发有限公司、广州市顺天计算机科技有限公司、广州市开利网络科技有限公司、广州市安思柏科技有限公司、广州佰能信息科技有限公司、广联达科技股份有限公司、广东省深圳国泰安教育技术有限公司、广东联和信息技术有限公司、福州金网际软件开发有限公司、烽火通信科技股份有限公司、大连华天软件有限公司、创辉科技有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、缤刻普锐（北京）科技有限责任公司、北京中远麒麟科技有限公司、北京印象笔记科技有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京西窗文化传媒有限公司、北京数科网维技术有限责任公司、北京派网软件有限公司、北京诺春风医疗科技有限公司、北京慕华信息科技有限公司、北京谋智火狐信息技术有限公司、北京快手科技有限公司、北京京视健康科技有限公司、北京金钥匙凯丽科技发展有限公司、北京慧同科技有限公司、北京和利时集团、北京格胜科技有限公司、北京多夸克教育科技有限公司、北京点聚信息技术有限公司、北京点点医科技有限公司、北京大铁科技有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、保定市大为计算机软件开发有限公司、蚌埠市城投智慧停车管理有限公司、百度安全应急响应中心、安美世纪（北京）科技有限公司、安徽美图信息科技有限公司、阿里巴巴集团安全应急响应中心、ZZCMS 和 SEACMS。

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、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、西安四叶草信息技术有限公司等单位报送公开收集的漏洞数量较多。贵州泰若数字科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京升鑫网络科技有限公司、杭州迪普科技股份有限公司、快页信息技术有限公司、杭州默安科技有限公司、贵州多彩网安科技有限公司、安徽锋刃信息科技有限公司、北京山石网科信息技术有限公司、郑州埃文科技、博智安全科技股份有限公司、江苏保旺达软件技术有限公司、北京安盟信息技术股份有限公司、重庆都会信息科技有限公司、河南东方云盾信息技术有限公司、河南灵创电子科技有限公司、山东九域信息技术有限公司、中国工商银行股份有限公司软件开发中心、北京华顺信安信息技术有限公司、山东云天安全技术有限公司、上海齐同信息科技有限

公司、奇安星城网络安全运营服务（长沙）有限公司、重庆易阅科技有限公司、上海纽盾科技股份有限公司、苏州棱镜七彩信息科技有限公司、福建省海峡信息技术有限公司、北京六方云信息技术有限公司、上海银基信息安全技术股份有限公司、平安银河实验室、浙江木链物联网科技有限公司、安徽长泰科技有限公司、浙江信安昆仑信息技术有限公司、上海上讯信息技术股份有限公司、广州安亿信软件科技有限公司、北京君云天下科技有限公司、华鲁数智信息技术（北京）有限公司、北京微步在线科技有限公司、星云博创科技有限公司、北京安帝科技有限公司、山东正中信息技术股份有限公司、贵州电网有限责任公司信息中心、北京万户网络技术有限公司、教育部教育管理信息中心、国网湖北省电力有限公司恩施供电公司、上海天存信息技术有限公司、蚂蚁金服、广东唯顶信息科技股份有限公司及及其他个人白帽子向 CNVD 提交了 39112 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）、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 35342 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）	23709	23709
斗象科技（漏洞盒子）	10236	10236
上海交大	1256	1256
北京神州绿盟科技有限公司	1019	481
新华三技术有限公司	481	0
深信服科技股份有限公司	392	0
安天科技集团股份有限公司	271	0
西安四叶草信息技术有限公司	207	207
北京数字观星科技有限公司	153	0
南京众智维信息科技有限公司	146	146
三六零数字安全科技集团有限公司	141	141
北京启明星辰信息安	132	0

全技术有限公司		
阿里云计算有限公司	106	0
恒安嘉新（北京）科技股份公司	99	0
天津市国瑞数码安全系统股份有限公司	59	0
中国电信集团系统集成有限责任公司	29	0
北京知道创宇信息技术有限公司	31	0
深圳市腾讯计算机系统有限公司（玄武实验室）	21	21
内蒙古云科数据服务股份有限公司	17	17
杭州安恒信息技术股份有限公司	15	6
卫士通信息产业股份有限公司	13	13
北京天融信网络安全技术有限公司	7	7
北京长亭科技有限公司	4	4
北京信联科汇科技有限公司	1	1
贵州泰若数字科技有限公司	350	350
北京云科安信科技有限公司（Seraph 安全实验室）	303	303
北京升鑫网络科技有限公司	126	126
杭州迪普科技股份有限公司	115	115
快页信息技术有限公	44	44

司		
杭州默安科技有限公司	40	40
贵州多彩网安科技有限公司	22	22
安徽锋刃信息科技有限公司	18	18
北京山石网科信息技术有限公司	15	15
郑州埃文科技	14	14
博智安全科技股份有限公司	13	13
江苏保旺达软件技术有限公司	13	13
北京安盟信息技术股份有限公司	11	11
重庆都会信息科技有限公司	10	10
河南东方云盾信息技术有限公司	9	9
河南灵创电子科技有限公司	8	8
山东九域信息技术有限公司	8	8
中国工商银行股份有限公司软件开发中心	6	6
北京华顺信安信息技术有限公司	6	6
山东云天安全技术有限公司	5	5
上海齐同信息科技有限公司	4	4
奇安星城网络安全运营服务（长沙）有限公司	4	4

重庆易阅科技有限公司	3	3
上海纽盾科技股份有限公司	3	3
苏州棱镜七彩信息科技有限公司	3	3
福建省海峡信息技术有限公司	3	3
北京六方云信息技术有限公司	2	2
上海银基信息安全技术股份有限公司	2	2
平安银河实验室	2	2
浙江木链物联网科技有限公司	2	2
安徽长泰科技有限公司	2	2
浙江信安昆仑信息技术有限公司	2	2
上海上讯信息技术股份有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京君云天下科技有限公司	2	2
华鲁数智信息技术（北京）有限公司	2	2
北京微步在线科技有限公司	2	2
星云博创科技有限公司	2	2
北京安帝科技有限公司	1	1
山东正中信息技术股份有限公司	1	1

贵州电网有限责任公司信息中心	1	1
北京万户网络技术有限公司	1	1
教育部教育管理信息中心	1	1
国网湖北省电力有限公司恩施供电公司	1	1
上海天存信息技术有限公司	1	1
蚂蚁金服	1	1
广东唯顶信息科技股份有限公司	1	1
CNCERT 内蒙古分中心	7	7
CNCERT 湖南分中心	5	5
CNCERT 浙江分中心	1	1
个人	1665	1665
报送总计	41412	39112

本周漏洞按类型和厂商统计

本周，CNVD 收录了 536 个漏洞。WEB 应用 255 个，应用程序 181 个，网络设备（交换机、路由器等网络端设备）55 个，智能设备（物联网终端设备）19 个，操作系统 19 个，安全产品 5 个，数据库 2 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	255
应用程序	181
网络设备（交换机、路由器等网络端设备）	55
智能设备（物联网终端设备）	19
操作系统	19
安全产品	5
数据库	2

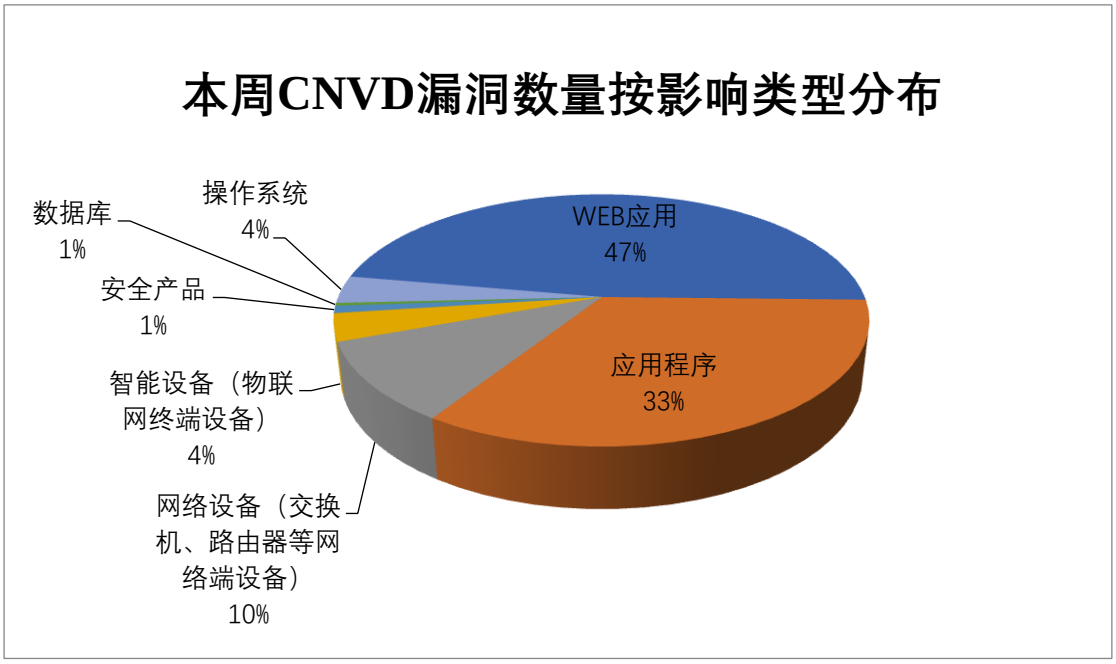

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Jenkins、Google、Adobe 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	Jenkins	24	5%
2	Google	20	4%
3	Adobe	19	4%
4	Apache	17	3%
5	F5	11	2%
6	Samsung	8	1%
7	新华三技术有限公司	8	1%
8	LibreNMS	7	1%
9	Huawei	6	1%
10	其他	416	78%

本周行业漏洞收录情况

本周，CNVD 收录了 36 个电信行业漏洞，30 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Huawei EMUI 和 Magic UI 信息泄露漏洞（CNVD-2022-81251）、Elcomplus SmartPPT 文件上传漏洞”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/

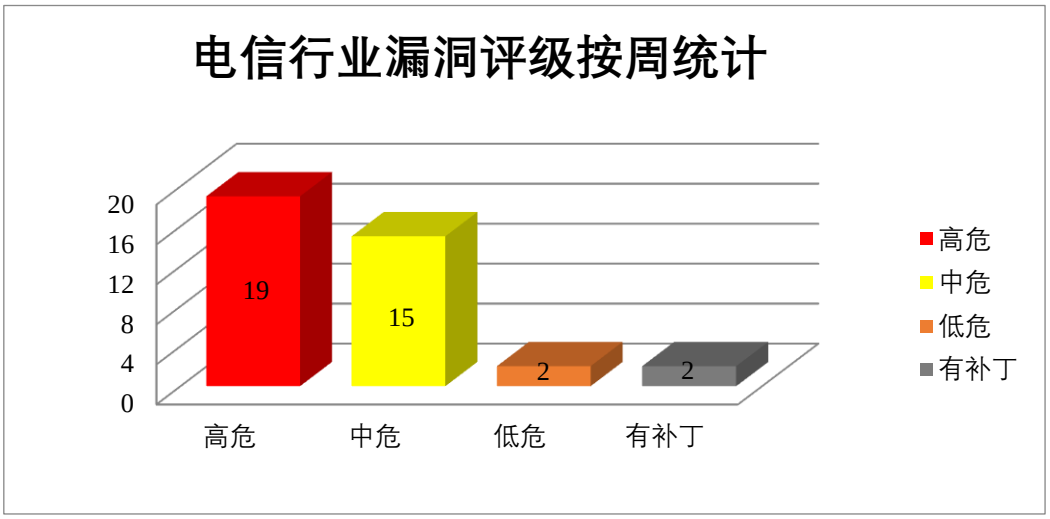

图 3 电信行业漏洞统计

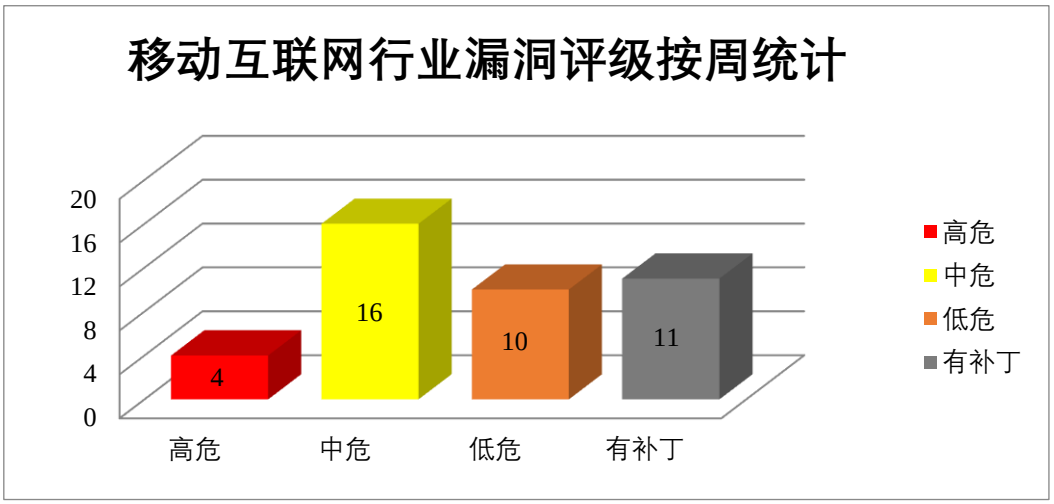

图 4 移动互联网行业漏洞统计

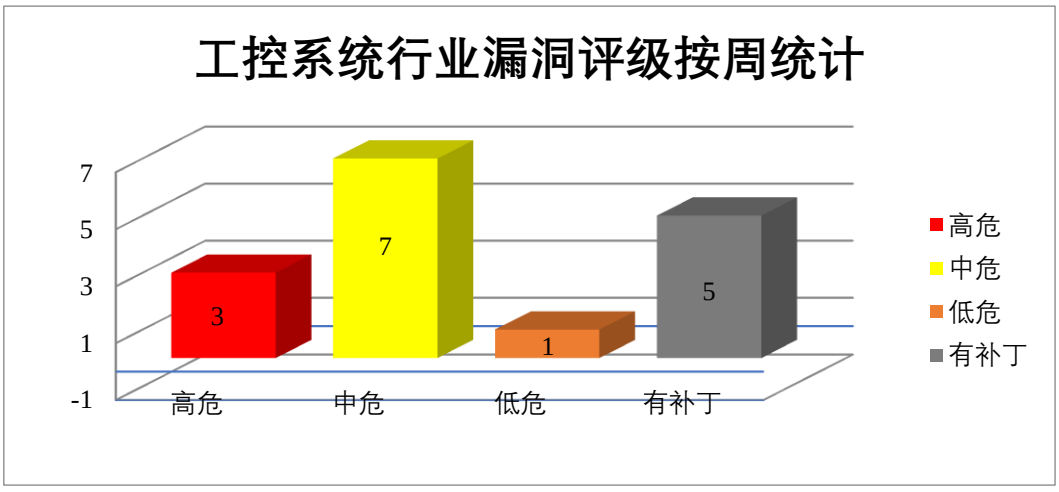

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Dimension 是美国 Adobe 公司的一套 2D 和 3D 合成设计工具。Adobe InDesign 是一套排版编辑应用程序。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。

CNVD 收录的相关漏洞包括：Adobe Dimension 内存错误引用漏洞（CNVD-2022-78869）、Adobe Dimension 越界读取漏洞（CNVD-2022-78868）、Adobe InDesign 越界读取漏洞（CNVD-2022-79424、CNVD-2022-79423）、Adobe InDesign 堆缓冲区溢出漏洞（CNVD-2022-79412、CNVD-2022-79422、CNVD-2022-79425）、Adobe InDesign 越界写入漏洞（CNVD-2022-79413）。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-2022-78869
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78868
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79412
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79413
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79422
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79424
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79423
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79425

2、 Apache 产品安全漏洞

Apache SOAP 是美国阿帕奇（Apache）基金会的一个可用作客户端库来调用其他地方可用的 SOAP 服务，也可以用作服务器端工具来实现 SOAP 可访问服务。Apache Airflow 是一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。Apache DolphinScheduler 是一个分布式的基于 DAG 可视化的工作流任务调度系统。Apache InLong 是一站式的海量数据集成框架，提供自动化、安全、可靠的数据传输能力。Apache MINA 是一款网络应用程序框架，该产品主要用于开发高性能和高可伸缩性的网络应用程序。Apache Dubbo 是一款基于 Java 的轻量级 RPC（远程过程调用）框架，该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。Velocity Engine 是用于 Web 开发的基于 Java 的模板引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞触发 DAGs，通过手动提供 run_id 参数执行任意命令，通过日志服务器读取任何文件等。

CNVD 收录的相关漏洞包括：Apache SOAP 身份验证错误漏洞、Apache Airflow 信息泄露漏洞（CNVD-2022-78863）、Apache Airflow 代码注入漏洞、Apache Dolphin Scheduler 路径遍历漏洞、Apache InLong 反序列化漏洞、Apache MINA 反序列化漏洞、

Apache Dubbo 反序列化漏洞、Apache Velocity Engine 代码执行漏洞。其中，除“Apache DolphinScheduler 路径遍历漏洞”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-2022-78864
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78863
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78862
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78866
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79657
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79656
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79660
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79663

3、Google 产品安全漏洞

Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。Google Chrome 是一款 Web 浏览器。Google Android 是一套以 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，攻击者可利用漏洞导致程序崩溃，任意代码执行，蓝牙设置中的权限升级等。

CNVD 收录的相关漏洞包括：Google TensorFlow 缓冲区溢出漏洞（CNVD-2022-80680、CNVD-2022-80683）、Google TensorFlow 代码问题漏洞（CNVD-2022-80685）、Google Chrome 资源管理错误漏洞（CNVD-2022-81239、CNVD-2022-81238、CNVD-2022-81243）、Google Android 权限提升漏洞（CNVD-2022-81237）、Google Chrome Internals 堆缓冲区溢出漏洞。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-2022-80680
https://www.cnvd.org.cn/flaw/show/CNVD-2022-80683
https://www.cnvd.org.cn/flaw/show/CNVD-2022-80685
https://www.cnvd.org.cn/flaw/show/CNVD-2022-81239
https://www.cnvd.org.cn/flaw/show/CNVD-2022-81238
https://www.cnvd.org.cn/flaw/show/CNVD-2022-81237
https://www.cnvd.org.cn/flaw/show/CNVD-2022-81243
https://www.cnvd.org.cn/flaw/show/CNVD-2022-81240

4、F5 产品安全漏洞

F5 BIG-IP 和 F5 BIG-IP Guided Configuration（GC）都是美国 F5 公司的产品。F5 BIG-IP 是一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付

平台。F5 BIG-IP Guided Configuration 是一个配置模板。F5 BIG-IP AFM 是一款用于防护 DDos 攻击的高级防火墙产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在 BIG-IP 系统上造成拒绝服务，在当前登录用户的上下文中运行 JavaScript，上传恶意制作的文件，执行任意命令等。

CNVD 收录的相关漏洞包括：F5 BIG-IP 输入验证错误漏洞（CNVD-2022-79943）、F5 BIG-IP 代码问题漏洞（CNVD-2022-79944、CNVD-2022-79947）、F5 BIG-IP 多款产品跨站脚本漏洞、F5 BIG-IP 日志信息泄露漏洞、F5 BIG-IP 资源管理错误漏洞（CNVD-2022-79953）、F5 BIG-IP 安全特征问题漏洞、F5 BIG-IP AFM 代码问题漏洞。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-2022-79943
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79944
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79950
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79948
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79947
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79953
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79952
https://www.cnvd.org.cn/flaw/show/CNVD-2022-79951

5、D-Link DIR-823G 命令执行漏洞

D-Link DIR-823G 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-823G 被披露存在命令执行漏洞。攻击者可利用该漏洞导致任意命令执行。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-2022-81491

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-2022-78867	Adobe Illustrator 缓冲区溢出漏洞（CNVD-2022-78867）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/illustrator/apsb22-56.html
CNVD-2022-79884	MISP 反序列化漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/MISP/MISP/commit/93821c0de6a7dd32262ce62212773f43136ca66e

CNVD-2022-79893	Webtareas 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://sourceforge.net/projects/webtareas/
CNVD-2022-79912	Ed01-Cms SQL 注入漏洞（CNVD-2022-79912）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/chilin89117/ED01-CMS/issues/4
CNVD-2022-79916	TYPO3 One is Enough Library 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：http://typo3.org/security/advisory/typo3-ext-sa-2022-007/
CNVD-2022-79917	TYPO3 Seminar Manager 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：http://typo3.org/security/advisory/typo3-ext-sa-2022-006/
CNVD-2022-80679	Google TensorFlow 代码问题漏洞（CNVD-2022-80679）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xxcj-rhqg-m46g
CNVD-2022-80686	Doufox 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/farliy-hacker/Doufoxcms/issues/1
CNVD-2022-80698	LibreNMS 代码问题漏洞（CNVD-2022-80698）	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/librenms/librenms/commit/ce8e5f3d056829bfa7a845f9dc2757e21e419ddc
CNVD-2022-80696	Google TensorFlow 缓冲区溢出漏洞（CNVD-2022-80696）	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-w58w-79xv-6vcj

小结：本周，Adobe 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。此外，Apache、Google、F5 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致程序崩溃，上传恶意制作的文件，执行任意命令，通过日志服务器读取任何文件等。另外，D-Link DIR-823G 被披露存在命令执行漏洞。攻击者可利用该漏洞导致任意命令执行。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、Radare2 缓冲区溢出漏洞（CNVD-2022-81355）

验证描述

Radare2 是一套用于处理二进制文件的库和工具。

Radare2 5.6.8 之前版本存在缓冲区溢出漏洞，该漏洞源于 r_bin_ne_get_relocs 函数中读取越界，攻击者可利用该漏洞读取敏感信息或导致崩溃。

验证信息

POC 链接：https://huntr.dev/bounties/52b57274-0e1a-4d61-ab29-1373b555fea0/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-81355

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. “去中心化版 Twitter”Mastodon 曝出安全漏洞

安全研究员 Lenin Alevski 警告说社交媒体平台 Mastodon 的多个实例容易受到系统配置问题的影响。

参考链接：https://www.secrss.com/articles/49338

2. 专家发布了针对 macOS 沙箱逃逸漏洞的 PoC 利用代码

一位研究人员发布了 macOS 沙盒逃逸漏洞的详细信息和概念验证（PoC）代码，该漏洞被追踪为 CVE-2022-26696。

参考链接：https://securityaffairs.co/wordpress/138815/hacking/macos-sandbox-escape-flaw.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