国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 05 月 23 日-2022 年 05 月 29 日 **2022 年第 21 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 460 个，其中高危漏洞 165 个、中危漏洞 274 个、低危漏洞 21 个。漏洞平均分值为 6.04。本周收录的漏洞中，涉及 0day 漏洞 394 个（占 86%），其中互联网上出现“、Covid-19 Travel Pass Management System 任意文件删除漏洞、Merchandise Online Store 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 11141 个，与上周（8507 个）环比增加 31%。

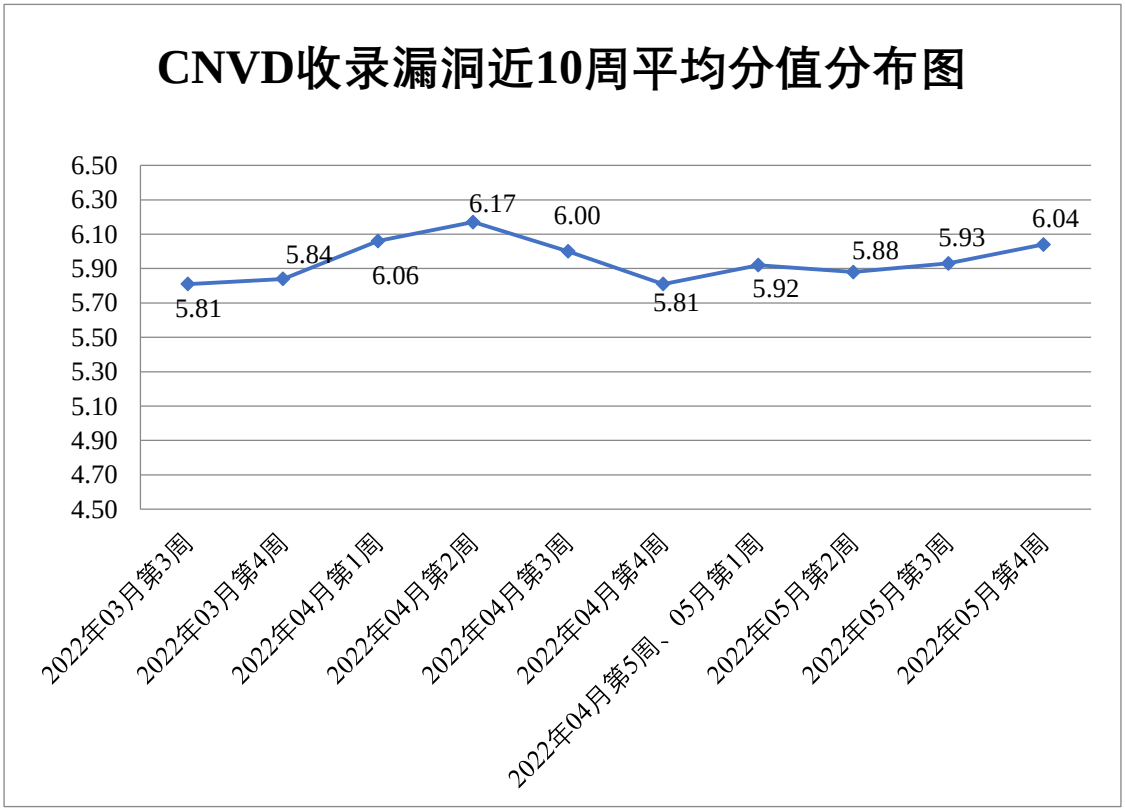

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 40 起，向基础电信企业通报漏洞事件 56 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 711 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 59 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 137 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、珠海金山办公软件有限公司、珠海奔图电子有限公司、重庆梅安森科技股份有限公司、重庆国翰能源发展有限公司、浙江自贸区耀光网络科技有限公司、浙江臻善科技股份有限公司、浙江大华技术股份有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、优慕课在线教育科技（北京）有限责任公司、用友网络科技股份有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、西安瑞友信息技术资讯有限公司、武汉云贝网络科技有限公司、武汉木仓科技股份有限公司、武汉达梦数据库股份有限公司、维沃移动通信有限公司、微软（中国）有限公司、网件（北京）网络技术有限公司、天津东洋油墨有限公司、太原迅易科技有限公司、索尼（中国）有限公司、苏州科达科技股份有限公司、苏州汇川技术有限公司、四平市九州易通科技有限公司、思科系统（中国）网络技术有限公司、视联动力信息技术股份有限公司、施耐德电气（中国）有限公司、深圳昱途网络科技有限公司、深圳市四海众联网络科技有限公司、深圳市吉祥腾达科技有限公司、深圳极速创想科技有限公司、深圳华望技术有限公司、深信服科技股份有限公司、上海曼恒数字技术股份有限公司、上海宽娱数码科技有限公司、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、熵基科技股份有限公司、山西供销农芯乐电子商务有限公司、山东康程信息科技有限公司、厦门美图网科技有限公司、普联技术有限公司、南京中卫信软件科技股份有限公司、南京尚网网络科技有限公司、南京九则软件科技有限公司、墨客科技（深圳）有限公司、廊坊市极致网络科技有限公司、吉翁电子（深圳）有限公司、湖南快乐阳光互动娱乐传媒有限公司、湖南翱云网络科技有限公司、红旗智行科技（北京）有限公司、杭州中宝科技有限公司、杭州益仕行信息技术有限公司、杭州新中大科技股份有限公司、杭州美迪网络技术有限公司、杭州吉拉科技有限公司、杭州恒生数字设备科技有限公司、杭州荷花软件有限公司、汉诚信息技术（上海）有限公司、贵州觅新科技有限公司、广州网易计算机系统有限公司、广州同鑫科技有限公司、广州市中崎商业机器股份有限公司、广西装小匠网络科技有限公司、广西南宁领众网络科技有限公司、福州富昌维控电子科技有限公司、飞塔信息科技（北京）有限公司、飞狐信息技术（天津）有限公司、鼎捷软件股份有限公司、成都极米科技股份有限

公司、畅捷通信息技术股份有限公司、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、北京网测科技有限公司、北京三快在线科技有限公司 、北京润乾信息系统技术有限公司、北京人大金仓信息技术股份有限公司、北京趣拿软件科技有限公司、北京启泰天成科技有限公司、北京派网软件有限公司、北京墨迹风云科技股份有限公司、北京陌陌科技有限公司、北京良精志诚科技有限责任公司、北京酷我科技有限公司、北京九思协同软件有限公司、北京辰信领创信息技术有限公司、北京车之家信息技术有限公司、北京爱奇艺科技有限公司、安徽旭帆信息科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、阿里巴巴集团安全应急响应中心、百度安全应急响应中心、Zebra、WordPress、WDJA、WAGO、VMware, Inc.、TRENDnet、The Apache Software Foundation、RockMongo、Redis、QNO、PHPWind、NGINX、Joomla、Fronius、Eclipse、Catfish CMS 和 Adobe。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、新华三技术有限公司、北京数字观星科技有限公司、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。杭州迪普科技股份有限公司、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、长春嘉诚信息技术股份有限公司、广州百蕴启辰科技有限公司、武汉安域信息安全技术有限公司、山东云天安全技术有限公司、南京树安信息技术有限公司、北方实验室（沈阳）股份有限公司、快页信息技术有限公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、华鲁数智信息技术（北京）有限公司、苏州棱镜七彩信息科技有限公司、河南灵创电子科技有限公司、广州竞远安全技术股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京冠程科技有限公司、浙江大学控制科学与工程学院、贵州泰若数字科技有限公司、浙江木链物联网科技有限公司、武汉非尼克斯软件技术有限公司、上海纽盾科技股份有限公司、浙江大华技术股份有限公司、北京平凯星辰科技发展有限公司、广州安亿信软件科技有限公司、北京华云安信息技术有限公司、巨鹏信息科技有限公司、北京机沃科技有限公司、中通服咨询设计研究院有限公司、山石网科通信技术股份有限公司其他个人白帽子向 CNVD 提交了 11141 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）、三六零数字安全科技集团有限公司、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 8943 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）	5751	5751

三六零数字安全科技集团有限公司	1383	1383
斗象科技（漏洞盒子）	1279	1279
深信服科技股份有限公司	949	0
上海交大	530	530
新华三技术有限公司	307	0
北京数字观星科技有限公司	267	0
北京神州绿盟科技有限公司	230	5
安天科技集团股份有限公司	226	0
北京天融信网络安全技术有限公司	214	15
京东科技信息技术有限公司	194	125
杭州安恒信息技术股份有限公司	143	42
恒安嘉新（北京）科技股份公司	100	0
北京启明星辰信息安全技术有限公司	65	2
天津市国瑞数码安全系统股份有限公司	59	0
西安四叶草信息技术有限公司	56	56
南京众智维信息科技有限公司	45	45
内蒙古云科数据服务股份有限公司	35	35
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	17	5

卫士通信息产业股份有限公司	16	2
远江盛邦（北京）网络安全科技股份有限公司	14	14
南京联成科技发展股份有限公司	6	6
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
沈阳东软系统集成工程有限公司	1	1
北京华顺信安科技有限公司	273	0
杭州迪普科技股份有限公司	30	1
墨菲未来科技（北京）有限公司	18	0
北京山石网科信息技术有限公司	18	18
重庆都会信息科技有限公司	15	15
长春嘉诚信息技术股份有限公司	15	15
广州百蕴启辰科技有限公司	9	9
武汉安域信息安全技术有限公司	6	6
山东云天安全技术有限公司	5	5
南京树安信息技术有限公司	5	5
北方实验室（沈阳）股份有限公司	4	4
快页信息技术有限公	3	3

司		
北京天地和兴科技有限公司	3	3
河南信安世纪科技有限公司	3	3
华鲁数智信息技术（北京）有限公司	3	3
苏州棱镜七彩信息科技有限公司	3	3
河南灵创电子科技有限公司	3	3
广州竞远安全技术股份有限公司	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
北京冠程科技有限公司	2	2
浙江大学控制科学与工程学院	2	2
贵州泰若数字科技有限公司	2	2
浙江木链物联网科技有限公司	2	2
武汉非尼克斯软件技术有限公司	2	2
上海纽盾科技股份有限公司	2	2
浙江大华技术股份有限公司	1	1
北京平凯星辰科技发展有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京华云安信息技术	1	1

有限公司		
巨鹏信息科技有限公司	1	1
北京机沃科技有限公司	1	1
中通服咨询设计研究院有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 浙江分中心	11	11
CNCERT 宁夏分中心	2	2
CNCERT 青海分中心	1	1
个人	1710	1710
报送总计	14081	11141

本周漏洞按类型和厂商统计

本周，CNVD 收录了 460 个漏洞。WEB 应用 244 个，应用程序 87 个，网络设备（交换机、路由器等网络端设备）72 个，智能设备（物联网终端设备）40 个，安全产品 8 个，数据库 6 个，操作系统 3 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	244
应用程序	87
网络设备（交换机、路由器等网络端设备）	72
智能设备（物联网终端设备）	40
安全产品	8
数据库	6
操作系统	3

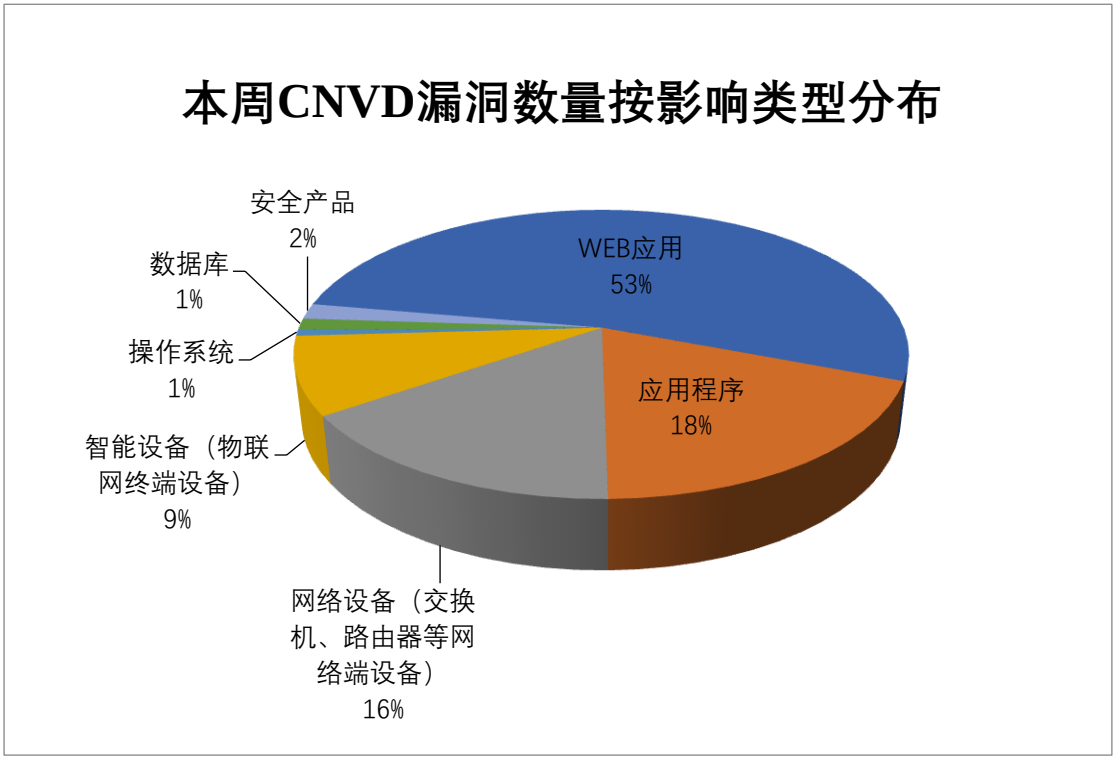

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Merchandise Online Store、WordPress 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	21	5%
2	Merchandise Online Store	16	4%
3	WordPress	16	4%
4	Brother	15	3%
5	SAP	13	3%
6	Apache	12	3%
7	深圳市必联电子有限公司	11	2%
8	D-Link	11	2%
9	Axis Communications AB	10	2%
10	其他	335	72%

本周行业漏洞收录情况

本周，CNVD 收录了 52 个电信行业漏洞，19 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“TOTOLINK N600R 存在命令执行漏洞、Google Android CarSetings 权限提升漏洞”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/

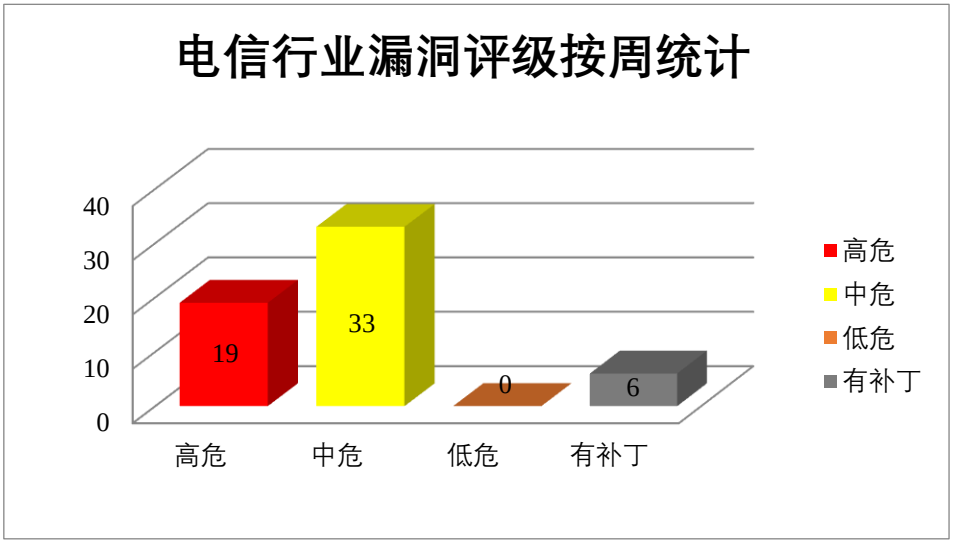

图 3 电信行业漏洞统计

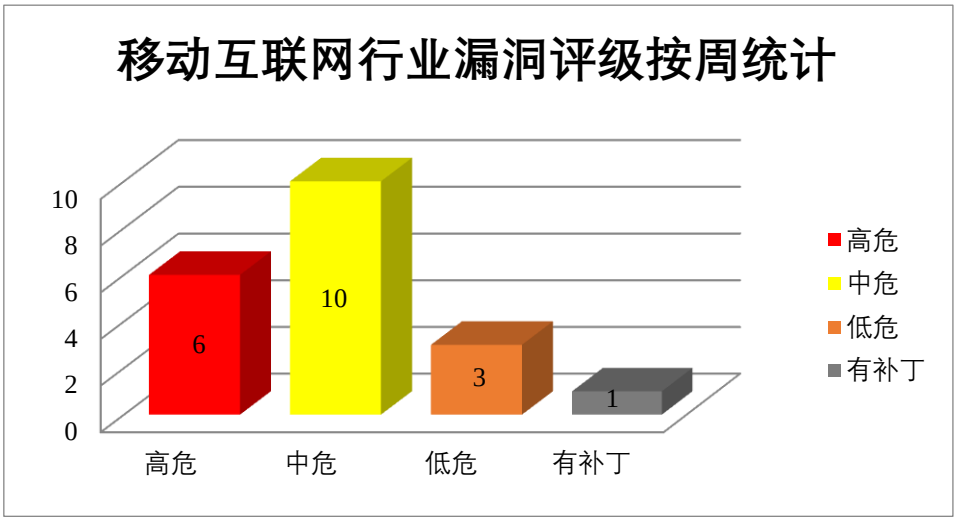

图 4 移动互联网行业漏洞统计

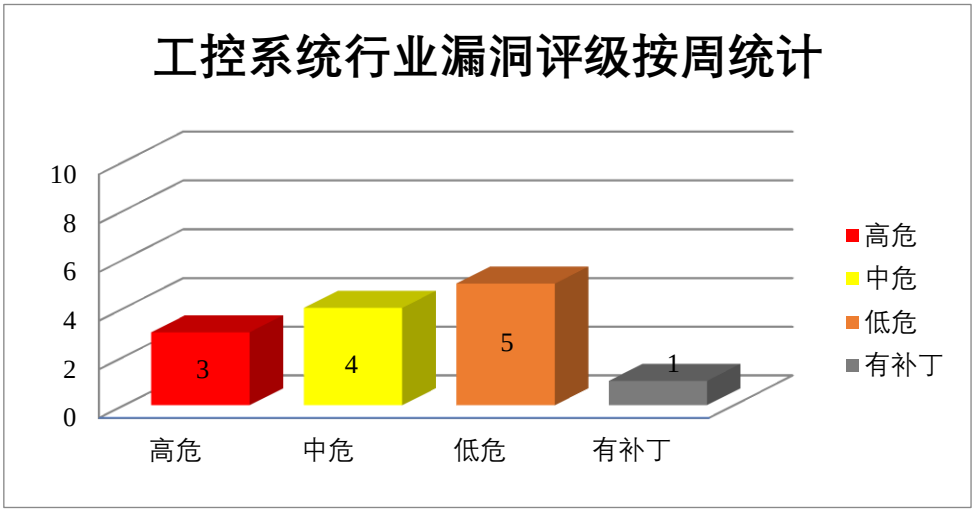

图 5 工控系统行业漏洞统计

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、SAP 产品安全漏洞

SAP Web dispatcher 是 Load Balancing 的核心组件，支持负载均衡，提供反向代理的功能，使得外网用户可以访问到内部应用。SAP Internet Communication Manager 是一个 SAP NetWeaver 应用程序服务器的组件。用于接收和发送 Web 请求（HTTP、HTTPS、SMTP）。SAP BusinessObjects Business Intelligence Platform 是德国思爱普（SAP）公司的一款完备的商务分析平台。该平台集市场领先的 SAP 数据整合产品、数据管理产品和商务智能 (BI) 产品于一身，可消除系统集成难题，快速、轻松地部署高性能的商务分析软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在客户端执行 JavaScript 代码，导致程序拒绝服务等。

CNVD 收录的相关漏洞包括：SAP Web Dispatcher 和 Internet Communication Manager 缓冲区溢出漏洞、SAP Web Dispatcher 和 Internet Communication Manager 拒绝服务漏洞、SAP NetWeaver Application Server 权限提升漏洞、SAP BusinessObjects Business Intelligence Platform XML 外部实体注入漏洞、SAP BusinessObjects Business Intelligence Platform 跨站脚本漏洞、SAP BusinessObjects Business Intelligence Platform 授权问题漏洞、SAP BusinessObjects Business Intelligence platform 信息泄露漏洞（CNVD-2022-41313、CNVD-2022-41312）。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-2022-41302

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41301

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41306

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41311

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41310

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41309

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41313

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41312

2、 Adobe 产品安全漏洞

Adobe Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。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执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Framemaker 越界写入漏洞（CNVD-2022-41732、CNVD-2022-41735、CNVD-2022-41734、CNVD-2022-41733、CNVD-2022-41737、CNVD-2022-41736、CNVD-2022-41740）、Adobe Framemaker 资源管理错误漏洞。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-2022-41732

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41735

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41734

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41733

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41737

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41736

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41741

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41740

3、 Apache 产品安全漏洞

Apache Doris 是美国阿帕奇（Apache）基金会的一个现代 MPP 分析数据库产品。可以提供亚秒级查询和高效的实时数据分析。Apache CouchDB 是美国阿帕奇（Apache）基金会的使用 Erlang 开发的一套面向文档的数据库系统。Apache Tika 是美国阿帕奇（Apache）基金会的一个集成了 POI（使用 Java 程序对 MicrosoftOffice 格式文档提供读和写功能的开源函数库）、Pdfbox（读取和创建 PDF 文档的纯 Java 类库）并为文本抽取工作提供了统一界面的内容抽取工具集合。Apache ShenYu 是美国阿帕奇（Apache）基金会的一个异步的，高性能的，跨语言的，响应式的 API 网关。Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。Apache DolphinScheduler 是美国阿帕奇（Apache）基金会开发的一个分布式去中心化，易扩展的可视化 DAG 工作流任务调度平台。致力于解决数据处理流程中错综复杂的依赖关系，使调度系统在数据处理

流程中开箱即用。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无效请求，获取和修改底层数据库中的信息，导致进程崩溃等。

CNVD 收录的相关漏洞包括：Apache Doris 信息泄露漏洞、Apache CouchDB 访问控制错误漏洞、Apache Tika 拒绝服务漏洞（CNVD-2022-41633）、Apache ShenYu 拒绝服务漏洞、Apache HTTP Server 拒绝服务漏洞（CNVD-2022-41639）、Apache Traffic Server 输入验证错误漏洞（CNVD-2022-41636）、Apache DolphinScheduler SQL 注入漏洞、Apache HTTP Server 缓冲区溢出漏洞（CNVD-2022-41640）。其中，“Apache CouchDB 访问控制错误漏洞、Apache HTTP Server 缓冲区溢出漏洞（CNVD-2022-41640）” 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-2022-41635
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41634
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41633
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41632
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41639
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41636
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41641
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41640

4、 WordPress 产品安全漏洞

WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞更改插件设置，在客户端执行 JavaScript 代码等。

CNVD 收录的相关漏洞包括：WordPress 插件 Easy Google Maps 跨站脚本漏洞、WordPress Ad Injection plugin 跨站脚本漏洞、WordPress Advanced Page Visit Counter plugin SQL 注入漏洞、WordPress Tripetto plugin 跨站脚本漏洞、WordPress DW Question & Answer Pro plugin 跨站请求伪造漏洞、WordPress DW Question & Answer Pro plugin 访问控制错误漏洞、WordPress Coming Soon by Supsystic plugin 跨站脚本漏洞、WordPress ShortPixel Adaptive Images plugin 访问控制错误漏洞。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-2022-41267
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41280
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41315
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41314
https://www.cnvd.org.cn/flaw/show/CNVD-2022-41318

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41317

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41316

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41321

5、D-Link DIR816L 远程代码执行漏洞

D-Link DIR816 是一款双频路由器。本周，D-Link DIR816L 被披露存在远程代码执行漏洞，该漏洞源于 shareport.php 的 value 参数未能正确过滤构造代码段的特殊元素。攻击者可利用此漏洞导致任意代码执行。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-2022-41743

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-2022-40233	Fastjson 远程代码执行漏洞（CNVD-2022-40233）	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/alibaba/fastjson/wiki/security_update_20220523
CNVD-2022-40308	TRENDnet TI-PG1284i 整数下溢漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.trendnet.com/support/view.asp?cat=4&id=81
CNVD-2022-40314	TRENDnet TI-PG1284i 整数下溢漏洞（CNVD-2022-40314）	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.trendnet.com/support/view.asp?cat=4&id=81
CNVD-2022-40317	Delta Electronics CNCSoft 堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft&sort_expr=cdate&sort_dir=DESC
CNVD-2022-41634	Apache CouchDB 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00
CNVD-2022-41640	Apache HTTP Server 缓冲区溢出漏洞（CNVD-2022-41640）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://httpd.apache.org/security/vulnerabilities_24.html
CNVD-2022	Adobe Framemaker 越界写入	高	目前厂商已发布升级补丁以修复漏

-41735	漏洞（CNVD-2022-41735）		洞，补丁获取链接：https://helpx.adobe.com/security/products/framemaker/apsb22-27.html
CNVD-2022-41734	Adobe Framemaker 越界写入漏洞（CNVD-2022-41734）	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/framemaker/apsb22-27.html
CNVD-2022-41738	Adobe Framemaker 资源管理错误漏洞（CNVD-2022-41738）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/framemaker/apsb22-27.html
CNVD-2022-41742	Google Android CarSetings 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/aaos/2022-05-01

小结：本周，SAP 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，在客户端执行 JavaScript 代码，导致程序拒绝服务等。此外，Adobe、Apache、WordPress 等多款产品被披露存在多个漏洞，攻击者可利用漏洞发送无效请求，获取和修改底层数据库中的信息，更改插件设置，在当前用户的上下文中执行任意代码，导致进程崩溃等。另外，D-Link DIR816 被披露存在远程代码执行漏洞，攻击者可利用此漏洞导致任意代码执行。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。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、 Covid-19 Travel Pass Management System 任意文件删除漏洞

验证描述

Covid-19 Travel Pass Management System 是一个 Covid-19 旅行通行证管理系统。为个人在 Covid-19 限制中提交旅行通行证提供了一个在线平台。

Covid-19 Travel Pass Management System 存在安全漏洞，该漏洞源于/ctpms/classes/Master.php?f=delete_img 缺少文件类型的检测。攻击者可利用漏洞删除任意文件。

验证信息

POC 链接：https://github.com/k0xx11/bug_report/blob/main/vendors/oretnom23/covid-19-travel-pass-management-system/delete-file-1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-40239

信息提供者

恒安嘉新（北京）科技股份公司

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. OAS 平台受 RCE 和 API 访问漏洞的影响

Bleeping Computer 网站消息，威胁分析专家披露开放自动化软件（OAS）平台存在安全漏洞，漏洞可导致设备访问、拒绝服务和远程代码执行。

参考链接：https://www.freebuf.com/news/334469.html

2. 新型 Zoom 漏洞：攻击者仅需要发送一条消息就可以发动攻击

视频会议服务软件 Zoom 解决了四个安全漏洞，这些漏洞可通过发送特别制作的可扩展信息和和执行恶意代码来攻击聊天中的其他用户。

参考链接：https://thehackernews.com/2022/05/new-zoom-flaws-could-let-attackers-hack.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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