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 16 日-2022 年 05 月 22 日 **2022 年第 20 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 462 个，其中高危漏洞 152 个、中危漏洞 273 个、低危漏洞 37 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 368 个（占 80%），其中互联网上出现“FUEL CMS 跨站脚本漏洞（CNVD-2022-38554）、ftcms 任意文件写入漏洞”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 8507 个，与上周（8445 个）环比增加 0.7%。

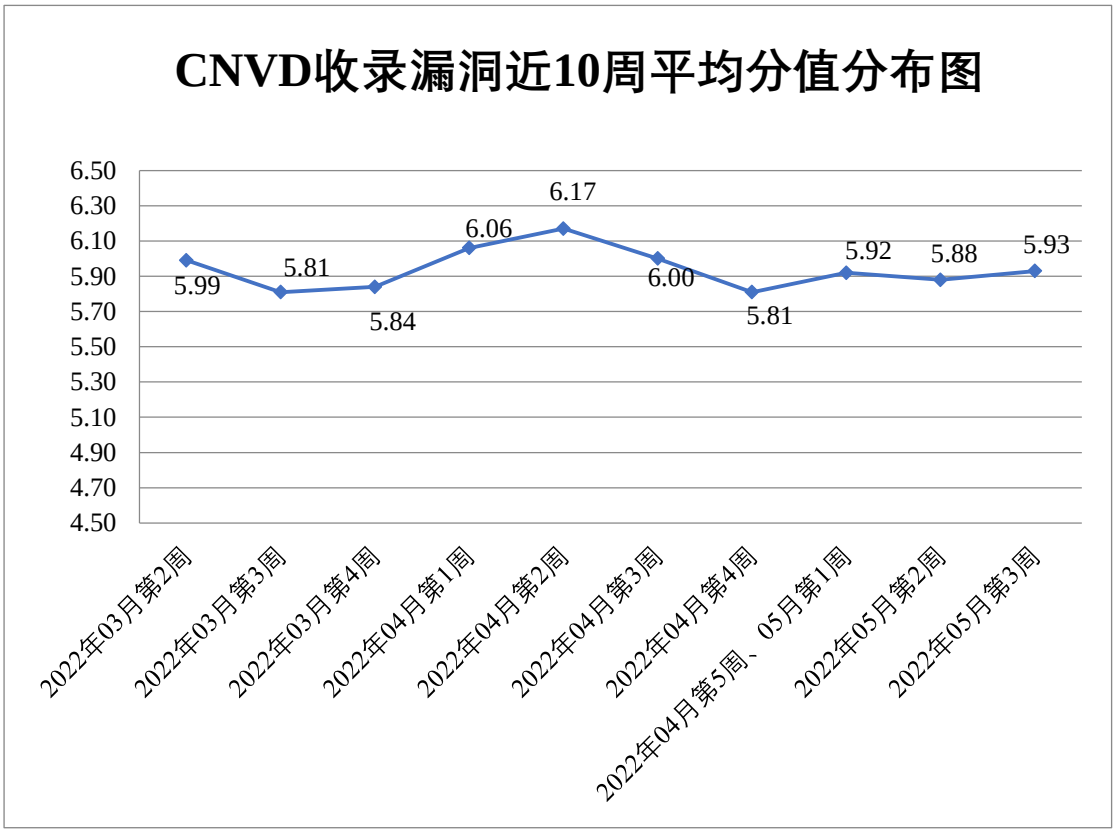

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 33 起，向基础电信企业通报漏洞事件 32 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 640 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 76 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 99 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：

中新网络信息安全股份有限公司、浙江臻善科技股份有限公司、浙江浙大中控信息技术有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、圆角科技发展（佛山）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、兄弟（中国）商业有限公司、夏普商贸（中国）有限公司、武汉中地数码科技有限公司、武汉海昌信息技术有限公司、武汉烽火信息集成技术有限公司、微软（中国）有限公司、网件（北京）网络技术有限公司、同望科技股份有限公司、天瑞仪器股份有限公司、唐山平升电子技术开发有限公司、太原迅易科技有限公司、四创科技有限公司、四川迅睿云软件开发有限公司、四川蓝光发展股份有限公司 、石基环企软件（苏州）有限公司、施耐德电气（中国）有限公司、深圳维盟科技股份有限公司、深圳市迅雷网络技术有限公司、深圳市迅捷通信技术有限公司、深圳市维斯易联科技有限公司、深圳市腾讯计算机系统有限公司、深圳市美科星通信技术有限公司、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、深圳市和为顺网络技术有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、深圳金三立视频科技股份有限公司、上海卓卓网络科技有限公司、上海优景智能科技股份有限公司、上海梦创双杨数据科技股份有限公司、上海肯特仪表股份有限公司、上海斐讯数据通信技术有限公司、上海方程软件科技有限公司、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、上海冰峰计算机网络技术有限公司、熵基科技股份有限公司、商派软件有限公司、陕西超拼网网络科技有限公司、山西企凝信息科技有限公司、山石网科通信技术（北京）有限公司、润申信息科技（上海）有限公司、青岛易软天创网络科技有限公司、青岛易联互动网络科技有限公司、普联技术有限公司、宁波江丰生物信息技术有限公司、南京恒点信息技术有限公司、南昌北创科技发展有限公司、廊坊市极致网络科技有限公司、金蝶软件（中国）有限公司、江下信息科技（惠州）有限公司、济南拓兴电子科技有限公司、华硕电脑（上海）有限公司、湖南康通电子股份有限公司、杭州天祎网络科技有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、广州银云信息科技有限公司、广州图创计算机软件开发有限公司、广州红帆科技有限公司、广联达科技股份有限公司、飞救医疗科技（北京）有限公司、东华医为科技有限公司、东莞市冬惊鱼网络科技有限公

司、大为计算机软件开发有限公司、成都生动网络科技有限公司、成都青软青之软件有限公司、成都极米科技股份有限公司、北京卓软在线信息技术有限公司、北京智邦国际软件技术有限公司、北京星网锐捷网络技术有限公司、北京拓尔思信息技术股份有限公司、北京三唐科技有限公司、北京九思协同软件有限公司、北京九华互联科技有限公司、北京火星高科数字科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、安徽青柿信息科技有限公司、爱普生（中国）有限公司、信呼、ZengCMS、yawcam、WordPress、The Apache Software Foundation、svnWebUI、MuYuCMS、MOBOTIX、MikroTik、Geovision、emlog 和 Bandisoft。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、新华三技术有限公司、杭州安恒信息技术股份有限公司、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、重庆都会信息科技有限公司、上海纽盾科技股份有限公司、山东新潮信息技术有限公司、联想集团、广州百蕴启辰科技有限公司、杭州海康威视数字技术股份有限公司、北京天地和兴科技有限公司、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、山石网科通信技术股份有限公司、江苏保旺达软件技术有限公司、河南信安世纪科技有限公司、江苏国泰新点软件有限公司、北方实验室（沈阳）股份有限公司、快页信息技术有限公司、北京东方通科技股份有限公司、河南灵创电子科技有限公司、武汉非尼克斯软件技术有限公司、上海天存信息技术有限公司、思而听网络科技有限公司、山东云天安全技术有限公司、北京远禾科技有限公司、智网安云（武汉）信息技术有限公司、北京山石网科信息技术有限公司、浙江大学控制科学与工程学院、浙江木链物联网科技有限公司、巨鹏信息科技有限公司、中科汇能科技有限公司、北京边界无限科技有限公司、北京小米科技有限责任公司、广州安亿信软件科技有限公司、山谷网安科技股份有限公司、南京禾盾信息科技有限公司、广州万方计算机科技有限公司、北京航空航天大学、工商银行、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 8507 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 5324 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
网神信息技术（北京）股份有限公司	3108	3108
上海斗象信息科技有限公司（漏洞盒子）	1947	1947

阿里云计算有限公司	520	0
新华三技术有限公司	511	0
杭州安恒信息技术股份有限公司	463	463
深信服科技股份有限公司	442	0
上海交大	269	269
安天科技集团股份有限公司	223	0
北京天融信网络安全技术有限公司	215	15
北京神州绿盟科技有限公司	173	0
恒安嘉新(北京)科技股份公司	108	0
西安四叶草信息技术有限公司	96	96
北京数字观星科技有限公司	78	0
北京启明星辰信息安全技术有限公司	71	6
天津市国瑞数码安全系统股份有限公司	59	0
内蒙古云科数据服务股份有限公司	42	42
中国电信集团系统集成有限责任公司	28	0
南京众智维信息科技有限公司	17	17
南京联成科技发展股份有限公司	16	16
北京长亭科技有限公司	7	7
沈阳东软系统集成工程有限公司	2	2

北京知道创宇信息技术有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
京东科技信息技术有限公司	1	1
贵州泰若数字科技有限公司	670	670
北京华顺信安科技有限公司	246	0
重庆都会信息科技有限公司	48	48
墨菲未来科技(北京)有限公司	39	0
上海纽盾科技股份有限公司	33	33
山东新潮信息技术有限公司	25	25
联想集团	21	21
广州百蕴启辰科技有限公司	18	18
杭州海康威视数字技术股份有限公司	16	16
北京天地和兴科技有限公司	14	14
杭州迪普科技股份有限公司	14	0
北京云科安信科技有限公司（Seraph 安全实验室）	12	12
北京升鑫网络科技有限公司	8	8
山石网科通信技术股份有限公司	8	8

江苏保旺达软件技术有限公司	6	6
河南信安世纪科技有限公司	5	5
江苏国泰新点软件有限公司	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司	4	4
亚信科技（成都）有限公司	4	0
北京东方通科技股份有限公司	3	3
河南灵创电子科技有限公司	3	3
武汉非尼克斯软件技术有限公司	3	3
上海天存信息技术有限公司	3	3
思而听网络科技有限公司	3	3
山东云天安全技术有限公司	2	2
北京远禾科技有限公司	2	2
智网安云（武汉）信息技术有限公司	2	2
北京山石网科信息技术有限公司	2	2
浙江大学控制科学与工程学院	2	2
浙江木链物联网科技有限公司	2	2
巨鹏信息科技有限公	2	2

司		
中科汇能科技有限公司	1	1
北京边界无限科技有限公司	1	1
北京小米科技有限责任公司	1	1
广州安亿信软件科技有限公司	1	1
山谷网安科技股份有限公司	1	1
南京禾盾信息科技有限公司	1	1
广州万方计算机科技有限公司	1	1
北京航空航天大学	1	1
中国工商银行	1	1
北京机沃科技有限公司	1	1
CNCERT 贵州分中心	4	4
CNCERT 四川分中心	3	3
CNCERT 河北分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	1571	1571
报送总计	11217	8507

本周漏洞按类型和厂商统计

本周，CNVD 收录了 462 个漏洞。WEB 应用 195 个，应用程序 106 个，网络设备（交换机、路由器等网络端设备）94 个，智能设备（物联网终端设备）54 个，操作系统 6 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	195
应用程序	106

网络设备（交换机、路由器等网络端设备）	94
智能设备（物联网终端设备）	54
操作系统	6
安全产品	5
数据库	2

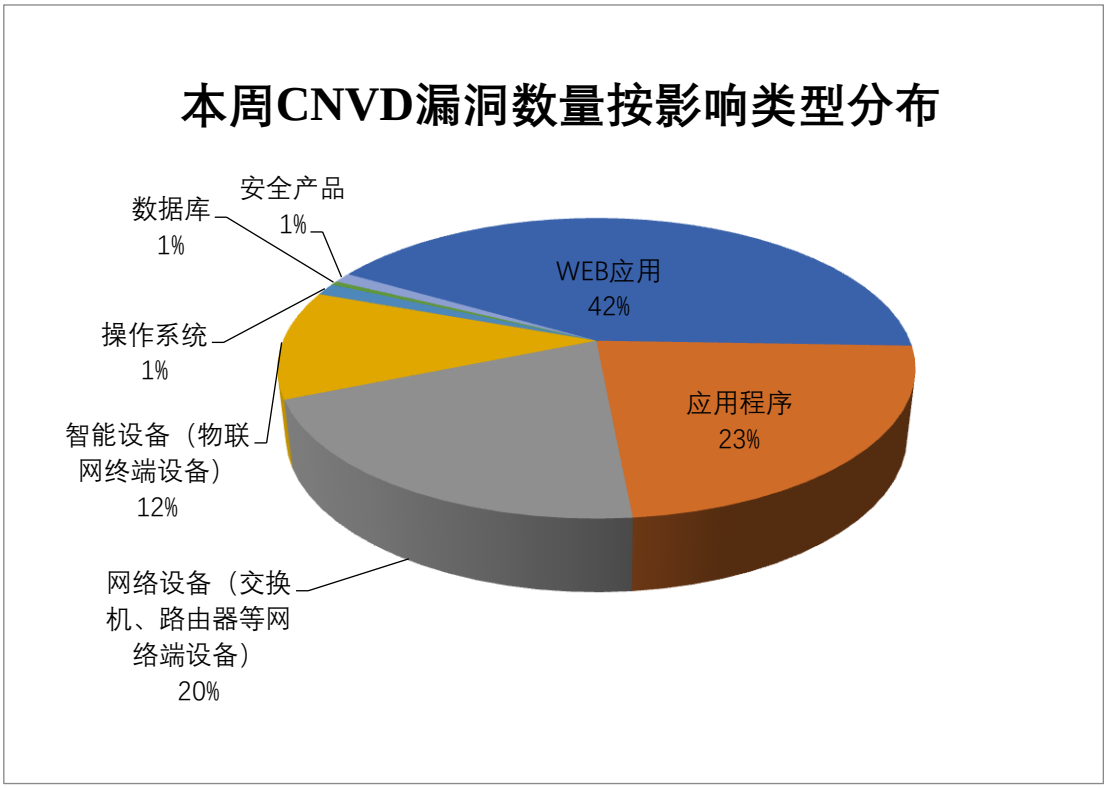

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Reolink、Tenda、D-Link 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	Reolink	29	6%
2	Tenda	15	3%
3	D-Link	14	3%
4	Apache	13	3%
5	IBM	12	3%
6	SECOMEA	10	2%
7	浙江自贸区耀光网络科技有限公司	8	2%
8	MOBOTIX	7	2%
9	Siemens	7	1%
10	其他	347	75%

本周行业漏洞收录情况

本周，CNVD 收录了 65 个电信行业漏洞，13 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，“D-Link DIR-823-Pro 命令注入漏洞（CNVD-2022-38531）、Tenda AX1806 堆栈溢出漏洞（CNVD-2022-38061）”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/

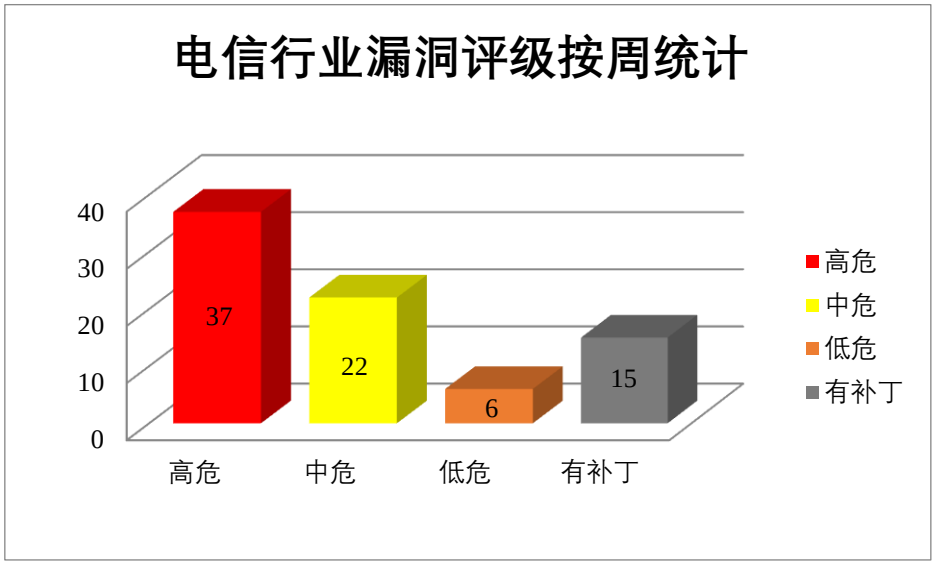

图 3 电信行业漏洞统计

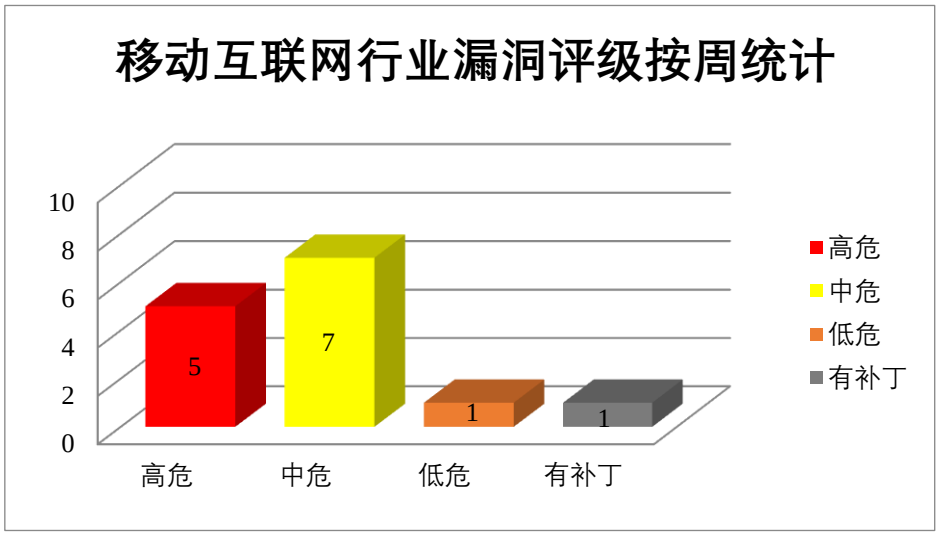

图 4 移动互联网行业漏洞统计

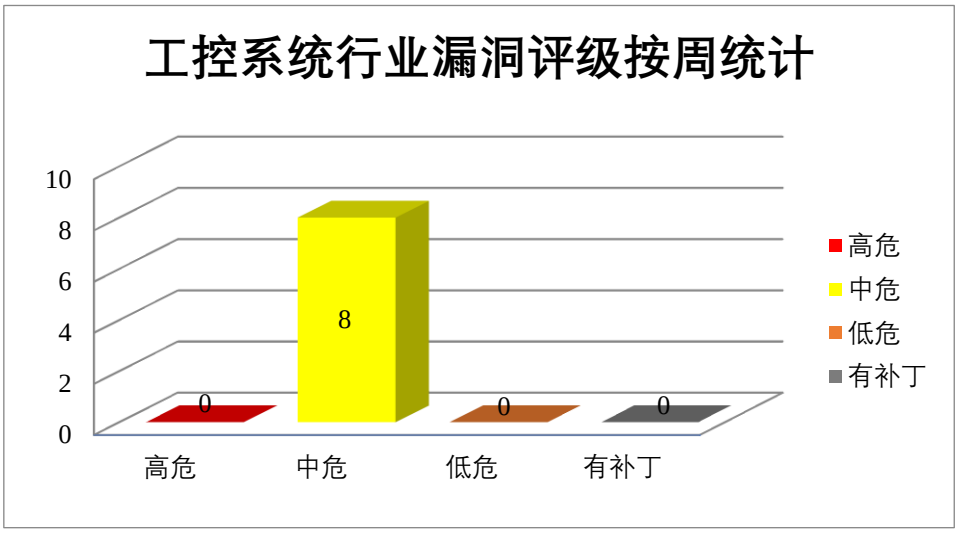

图 5 工控系统行业漏洞统计

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、D-Link 产品安全漏洞

D-Link DIR-823G 是中国台湾友讯（D-Link）公司的一款无线路由器。D-Link DIR-823-Pro 是一款路由器。D-Link DIR-846 是中国台湾友讯（D-Link）公司的一款无线路由器。D-Link DIR-878 是中国台湾友讯（D-Link）公司的一款无线路由器。D-Link Dir-X1860 是中国友讯（D-Link）公司的一款双频路由器。D-Link DIR-842 是台湾友讯科技股份有限公司生产的家用路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞实现命令注入，执行远程代码等。

CNVD 收录的相关漏洞包括：D-Link DIR-823G 命令注入漏洞（CNVD-2022-38532）、D-Link DIR-823-Pro 命令注入漏洞（CNVD-2022-38531）、D-Link DIR-846 命令执行漏洞、D-Link DIR-878 命令注入漏洞（CNVD-2022-38533）、D-Link Dir-X1860 拒绝服务漏洞（CNVD-2022-38536）、D-Link DIR-842 telnetd 认证防爆破保护机制绕过漏洞、D-Link DAP-1860 远程代码执行漏洞（CNVD-2022-38539、CNVD-2022-38538）。其中，除“D-Link Dir-X1860 拒绝服务漏洞（CNVD-2022-38536）D-Link DIR-842 telnetd 认证防爆破保护机制绕过漏洞”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-2022-38532

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38531

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38535

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38533

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38536

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38537

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38539

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38538

2、 Apache 产品安全漏洞

Apache Jena 是美国阿帕奇（Apache）基金会的一个 Java 语义网框架。用于构建语义 Web 和链接数据应用程序。Apache Superset 是一个现代的，工业级的 Business Intelligence 的 Web 应用。Apache Subversion 是美国阿帕奇（Apache）基金会的一套开源的版本控制系统。该系统可兼容并发版本系统(CVS)。Apache Apisix 是美国阿帕奇（Apache）基金会的一个云原生的微服务 API 网关服务。该软件基于 OpenResty 和 etcd 来实现，具备动态路由和插件热加载，适合微服务体系下的 API 管理。Apache James 是美国阿帕奇（Apache）基金会的一个完全用 Java 编写的开源 Smtp 和 Pop3 邮件传输代理和 Nntp 新闻服务器。Apache DolphinScheduler 是美国阿帕奇（Apache）基金会的一个分布式的基于 DAG 可视化的工作流任务调度系统。Apache Hadoop 是美国阿帕奇（Apache）基金会的一套开源的分布式系统基础架构。该产品能够对大量数据进行分布式处理，并具有高可靠性、高扩展性、高容错性等特点。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的 XML 文件读取文件，执行任意 SQL 语句，如查询数据、下载数据、写入 webshell、执行系统命令以及绕过登录限制等。

CNVD 收录的相关漏洞包括：Apache Jena XML 外部实体注入漏洞（CNVD-2022-38521）、Apache Superse SQL 注入漏洞、Apache Subversion 资源管理错误漏洞、Apache Apisix 信息泄露漏洞、Apache James 路径遍历漏洞（CNVD-2022-38529）、Apache DolphinScheduler 拒绝服务漏洞、Apache Hadoop 路径遍历漏洞、Apache Apisix 输入验证错误漏洞。其中，“Apache Jena XML 外部实体注入漏洞（CNVD-2022-38521）、Apache Superse SQL 注入漏洞、Apache Hadoop 路径遍历漏洞”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-2022-38521

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38526

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38524

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38523

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38529

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38528

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38527

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38530

3、 IBM 产品安全漏洞

IBM Sterling B2B Integrator 是美国 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 DataPower Gateway 是美国 IBM 公司的一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台。该平台可利用专用网关平台跨渠道保护、集成和优化访问。IBM Spectrum Virtualize 是美国 IBM 公司的一个块存储虚拟化系统。可提高新的和现有存储基础架构的数据价值、安全性和简单性。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM Robotic Process Automation 是美国 IBM 公司的一种机器人流程自动化产品。可帮助您以传统 RPA 的轻松和速度大规模自动化更多业务和 IT 流程。IBM Planning Analytics 是美国 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。Planning Analytics Workspace 是 IBM Planning Analytics 的 Web 管理界面。IBM InfoSphere Information Server 是一个数据集成软件平台。它的主要服务是帮助我们能理解、清理、监控、转换和交付数据。IBM Security Identity Manager（ISIM）是美国 IBM 公司的一套身份管理和治理解决方案。该方案可在整个用户生命周期内自动创建、修改、重新认证和终止用户特权，并支持基于策略的密码管理。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞可访问任意页面，将恶意可执行文件上传到系统中，可能会导致代码执行等。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 拒绝服务漏洞、IBM DataPower Gateway 拒绝服务漏洞（CNVD-2022-38547）、IBM Spectrum Virtualize 访问控制错误漏洞、IBM Maximo Asset Management 输入验证错误漏洞、IBM Robotic Process Automation 输入验证错误漏洞、IBM Planning Analytics Workspace 文件上传漏洞、IBM InfoSphere Information Server 权限提升漏洞（CNVD-2022-38557）、IBM Security Identity Manager 缓冲区溢出漏洞。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-2022-38548

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38547

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38552

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38555

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38553

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38559

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38557

https://www.cnvd.org.cn/flaw/show/CNVD-2022-38560

4、Tenda 产品安全漏洞

Tenda AX1806 是中国腾达（Tenda）公司的一款 WiFi6 无线路由器。Tenda AC15 是中国腾达（Tenda）公司的一款无线路由器。Tenda AC9 是中国腾达（Tenda）公司的一款无线路由器。Tenda AX12 是中国腾达（Tenda）公司的一款双频千兆 Wifi 6 无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务 (DoS)，导致堆栈溢出等。

CNVD 收录的相关漏洞包括：Tenda AX1806 堆栈溢出漏洞（CNVD-2022-38061、CNVD-2022-38064、CNVD-2022-38063、CNVD-2022-38065）、Tenda AC15 缓冲区溢出漏洞、Tenda AC15 命令注入漏洞、Tenda AC9 堆栈溢出漏洞（CNVD-2022-38540）、Tenda AX12 缓冲区溢出漏洞（CNVD-2022-38541）。其中，除“Tenda AC15 缓冲区溢出漏洞（CNVD-2022-38165）”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-2022-38061
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38064
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38063
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38065
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38165
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38164
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38540
https://www.cnvd.org.cn/flaw/show/CNVD-2022-38541

5、Tenda AC9 堆栈溢出漏洞（CNVD-2022-38543）

Tenda AC9 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC9 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞导致服务端栈溢出。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-2022-38543

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-2022-37791	OpenSSL 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2
CNVD-2022-38056	Piwigo cat_move.php SQL 注入漏洞	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：

			http://piwigo.org/
CNVD-2022-38153	squirrel SQL 注入漏洞	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/albertodemichelis/squirrel/commit/a6413aa690e0bdfef648c68693349a7b878fe60d
CNVD-2022-38166	cocoapods-downloader 命令注入漏洞	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/CocoaPods/cocoapods-downloader/pull/127
CNVD-2022-37371	Siemens Teamcenter 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://cert-portal.siemens.com/productcert/html/ssa-789162.html
CNVD-2022-38096	Atlassian Bitbucket Data Center 存在命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://confluence.atlassian.com/security/multiple-products-security-advisory-hazelcast-vulnerable-to-remote-code-execution-cve-2016-10750-1116292387.html
CNVD-2022-38254	Apache Spark 存在命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://github.com/apache/spark/commit/057c051285ec32c665fb458d0670c1c16ba536b2
CNVD-2022-38521	Apache Jena XML 外部实体注入漏洞（CNVD-2022-38521）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://lists.apache.org/thread/h88oh642455wljo0p5jgzs9phk4gj878
CNVD-2022-38061	Tenda AX1806 堆栈溢出漏洞（CNVD-2022-38061）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/product/AX1806.html
CNVD-2022-38064	Tenda AX1806 堆栈溢出漏洞（CNVD-2022-38064）	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.tenda.com.cn/product/AX1806.html

小结：本周，D-Link 产品被披露存在多个漏洞，攻击者可利用漏洞实现命令注入，执行远程代码等。此外，Apache、IBM、Tenda 等多款产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的 XML 文件读取文件，执行任意 SQL 语句，访问任意页面，将恶意可执行文件上传到系统中，可能会导致代码执行等。另外，Tenda AC9 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞导致服务端栈溢出。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、 FUEL CMS 跨站脚本漏洞（CNVD-2022-38554）

验证描述

FUEL CMS 是一款基于 Codelgniter 框架的内容管理系统（CMS）。

FUEL CMS 1.5.1 版本存在跨站脚本漏洞。该漏洞源于程序缺少对用户提供的数据和输出的数据校验过滤。攻击者可利用该漏洞在客户端执行 JavaScript 代码。

验证信息

POC 链接：https://github.com/daylightstudio/FUEL-CMS/issues/595

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-38554

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. 微软检测到 Linux XorDDoS 恶意软件活动激增

近期，微软表示在过去六个月中，一种用于入侵 Linux 设备并构建 DDoS 僵尸网络的隐秘模块化恶意软件的活动量大幅增加了 254%。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-detects-massive-surge-in-linux-xorddos-malware-activity/

2. 谷歌的 Java OAuth 客户端库报错

谷歌解决了其用于 Java OAuth 客户端库中的一个较严重性缺陷。

参考链接：https://thehackernews.com/2022/05/high-severity-bug-reported-in-googles.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