国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 10 月 17 日-2022 年 10 月 23 日 **2022 年第 42 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 449 个，其中高危漏洞 165 个、中危漏洞 235 个、低危漏洞 49 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 332 个（占 74%），其中互联网上出现“Wedding Planner select.php SQL 注入漏洞、ShopWind 跨站脚本漏洞”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漏洞总数 25769 个，与上周（14785 个）环比增加 74%。

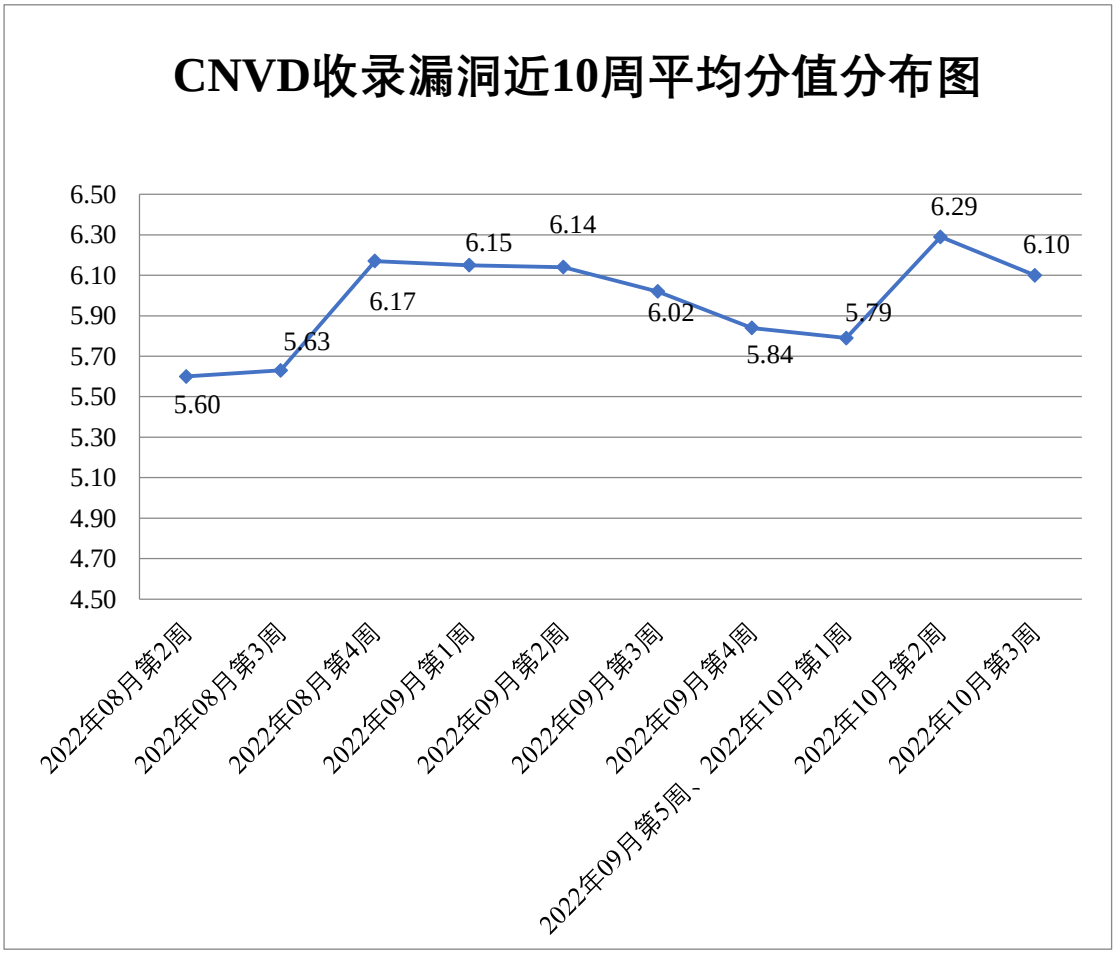

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 17 起，向基础电信企业通报漏洞事件 12 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 1077 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 156 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 77 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：

淄博闪灵网络科技有限公司、珠海高凌信息科技有限公司、重庆渝亿网络科技有限公司、重庆米未科技有限公司、郑州捷宸电子科技有限公司、正方软件股份有限公司、浙江兰德纵横网络技术股份有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、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、西安众邦网络科技有限公司、武汉烟岚科技有限公司、武汉光迅科技股份有限公司、潍坊奎文广文海宏软件开发中心、天津神州浩天科技有限公司、台达集团、速易购电子商务有限公司、苏州汇川技术有限公司、苏州国网电子科技有限公司、四川合美软件信息技术有限公司、深圳搜豹网络有限公司、深圳市正运动技术有限公司、深圳市研色科技有限公司、深圳市威纶通科技有限公司、深圳市思迅软件股份有限公司、深圳市科迈通讯技术有限公司、深圳市吉祥腾达科技有限公司、深圳市共济科技股份有限公司、深圳市必联电子有限公司、深圳昆仑通态科技有限责任公司、深圳创维数字技术有限公司、上海卓卓网络科技有限公司、上海迅时通信设备有限公司、上海茸易科技有限公司、上海荃路软件开发工作室、上海零分科技有限公司、上海凯聪电子科技有限公司、上海国云信息科技有限公司、上海孚盟软件有限公司、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、山东有人物联网股份有限公司、山东确信信息产业股份有限公司、厦门宇电自动化科技有限公司、厦门雅迅网络股份有限公司、厦门新页科技有限公司、厦门快商通科技股份有限公司、全讯汇聚网络科技（北京）有限公司、青果软件集团有限公司、青岛东胜伟业软件有限公司、千城云科（上海）数据科技有限公司、麒麟软件有限公司、欧姆龙自动化（中国）有限公司、南通润邦网络科技有限公司、南宁迈世信息技术有限公司、南方数据、美团安全应急响应中心、零视技术(上海)有限公司、联奕科技股份有限公司、力软信息技术（苏州）有限公司、理才云计算股份有限公司、乐星电气（无锡）有限公司、廊坊市极致网络科技有限公司、江西铭软科技有限公司、江苏邦宁科技有限公司、吉翁电子（深圳）有限公司、基恩士（中国）有限公司、惠普贸易（上海）有限公司、湖南康通电子股份

有限公司、湖南建研信息技术股份有限公司、恒锋信息科技股份有限公司、河南吉海网络科技有限公司、杭州易软共创网络科技有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、哈尔滨伟成科技有限公司、桂林思与云文化传媒有限公司、广州网易计算机系统有限公司、广州津虹网络传媒有限公司、广西南宁领众网络科技有限公司、广东卓锐软件有限公司、广东因行思智能科技有限公司、广东全程云科技有限公司、光环云数据有限公司、福建博思软件股份有限公司、东莞市通天星软件科技有限公司、成都星锐蓝海网络科技有限公司、成都九纪言科技有限公司、北京中科网威信息技术有限公司、北京中创视讯科技有限公司、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、北京小川科技有限公司、北京万户网络技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京天生创想信息技术有限公司、北京搜狐互联网信息服务有限公司、北京神州视翰科技有限公司、北京神州绿盟科技有限公司、北京龙软科技股份有限公司、北京猎鹰安全科技有限公司、北京康创安捷信息技术有限公司、北京九思协同软件有限公司、北京宏景世纪软件股份有限公司、北京抖音信息服务有限公司、北京鼎信创智科技有限公司、北京步鼎方舟科技有限公司、北京邦天信息技术有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京奥星贝斯科技有限公司、班安欧企业管理（上海）有限公司、安吉加加信息技术有限公司、安徽旭帆信息科技有限公司、艾默生网络能源有限公司和 ZZCMS。

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、深信服科技股份有限公司、新华三技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、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。北京升鑫网络科技有限公司、山东云天安全技术有限公司、浙江木链物联网科技有限公司、山东新潮信息技术有限公司、山石网科通信技术股份有限公司、星云博创科技有限公司、成方金融科技有限公司上海分公司、博智安全科技股份有限公司、河南东方云盾信息技术有限公司、长春嘉诚信息技术股份有限公司、苏州棱镜七彩信息科技有限公司、安徽锋刃信息科技有限公司、杭州美创科技有限公司、江苏省信息安全测评中心、中通服创发科技有限责任公司、北京六方云信息技术有限公司、广东唯顶信息科技股份有限公司、快页信息技术有限公司、广州安亿信软件科技有限公司、上海纽盾科技股份有限公司、中国工程物理研究院计算机应用研究所、成都安美勤信息技术股份有限公司、上海上讯信息技术股份有限公司、北京机沃科技有限公司、北京微步在线科技有限公司、华鲁数智信息技术（北京）有限公司、南京禾盾信息科技有限公司、北京航空航天大学、江西和尔惠信息技术有限公司、北京冠程科技有限公司及其他个人白帽子向 CNVD 提交了 25769 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23881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）	22363	22363
上海交大	1174	1174
北京神州绿盟科技有限公司	611	3
深信服科技股份有限公司	504	0
新华三技术有限公司	498	0
远江盛邦（北京）网络安全科技股份有限公司	382	382
奇安信网神（补天平台）	344	344
安天科技集团股份有限公司	263	0
北京数字观星科技有限公司	173	0
南京众智维信息科技有限公司	127	127
天津市国瑞数码安全系统股份有限公司	119	0
杭州安恒信息技术股份有限公司	115	115
恒安嘉新（北京）科技股份公司	107	6
北京天融信网络安全技术有限公司	99	5
北京启明星辰信息安全技术有限公司	69	8
中国电信集团系统集成有限责任公司	28	0
内蒙古云科数据服务	18	18

股份有限公司		
北京长亭科技有限公司	15	15
卫士通信息产业股份有限公司	9	9
西安四叶草信息技术有限公司	7	7
浙江大华技术股份有限公司	4	4
南京联成科技发展股份有限公司	4	4
西门子（中国）有限公司	1	0
北京知道创宇信息技术有限公司	1	0
北京升鑫网络科技有限公司	38	38
F5	18	0
山东云天安全技术有限公司	17	17
杭州迪普科技股份有限公司	15	0
浙江木链物联网科技有限公司	12	12
山东新潮信息技术有限公司	11	11
山石网科通信技术股份有限公司	10	10
星云博创科技有限公司	8	8
成方金融科技有限公司上海分公司	6	6
博智安全科技股份有限公司	6	6
河南东方云盾信息技	5	5

术有限公司		
长春嘉诚信息技术股份有限公司	5	5
苏州棱镜七彩信息科技有限公司	5	5
安徽锋刃信息科技有限公司	4	4
杭州美创科技有限公司	4	4
江苏省信息安全测评中心	4	4
中通服创发科技有限责任公司	4	4
北京六方云信息技术有限公司	3	3
广东唯顶信息科技股份有限公司	3	3
快页信息技术有限公司	3	3
广州安亿信软件科技有限公司	3	3
上海纽盾科技股份有限公司	2	2
中国工程物理研究院计算机应用研究所	2	2
北京华顺信安信息技术有限公司	2	0
成都安美勤信息技术股份有限公司	1	1
上海上讯信息技术股份有限公司	1	1
北京机沃科技有限公司	1	1
北京微步在线科技有限公司	1	1

华鲁数智信息技术（北京）有限公司	1	1
南京禾盾信息科技有限公司	1	1
北京航空航天大学	1	1
江西和尔惠信息技术有限公司	1	1
中国工商银行	1	1
北京冠程科技有限公司	1	1
CNCERT 贵州分中心	1	1
个人	1019	1019
报送总计	28255	25769

本周漏洞按类型和厂商统计

本周，CNVD 收录了 449 个漏洞。WEB 应用 195 个，应用程序 105 个，网络设备（交换机、路由器等网络端设备）89 个，操作系统 32 个，智能设备（物联网终端设备）16 个，安全产品 12 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	105
网络设备（交换机、路由器等网络端设备）	89
操作系统	32
智能设备（物联网终端设备）	16
安全产品	12

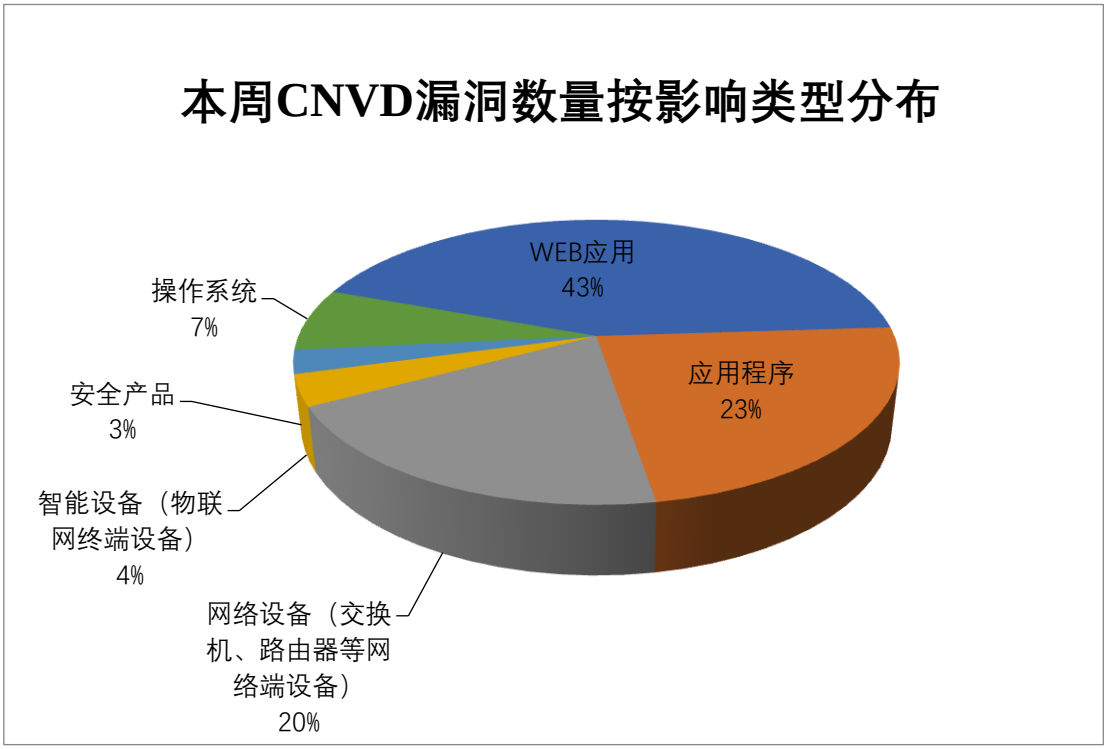

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、Microsoft、新华三技术有限公司等多家厂商的产品，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	Linux	24	5%
2	Microsoft	18	4%
3	新华三技术有限公司	17	4%
4	Apache	14	3%
5	用友网络科技股份有限公司	10	2%
6	OpenCats	10	2%
7	SAP	9	2%
8	TOTOLINK	9	2%
9	Tenda	8	2%
10	其他	330	74%

本周行业漏洞收录情况

本周，CNVD 收录了 62 个电信行业漏洞，10 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“TOTOLINK T8 存在缓冲区溢出漏洞（CNVD-2022-69723）、Samsung AppLinker 隐式意图劫持漏洞”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/

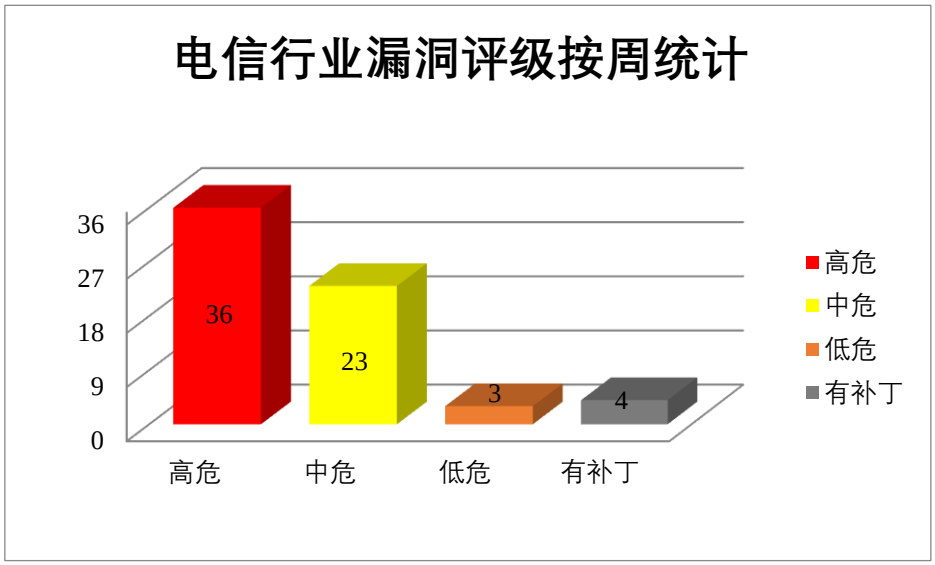

图 3 电信行业漏洞统计

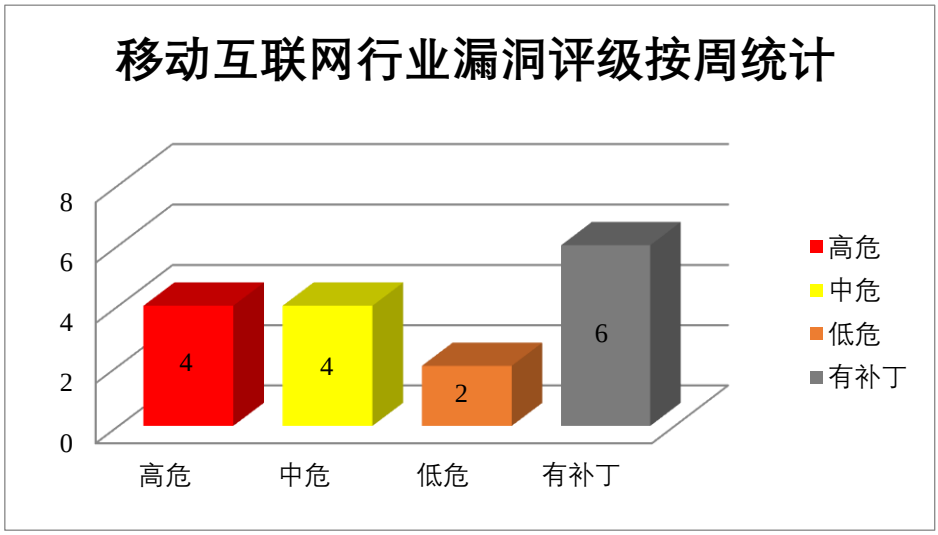

图 4 移动互联网行业漏洞统计

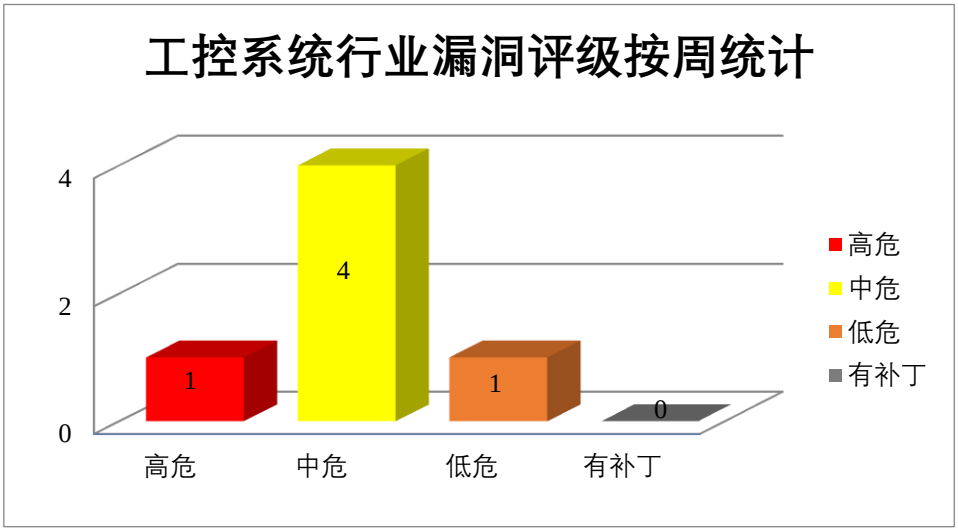

图 5 工控系统行业漏洞统计

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 NetWeaver AS 是德国思爱普（SAP）公司的一款 SAP 网络应用服务器。它不仅能提供网络服务，且还是 SAP 软件的基本平台。SAP 3D Visual Enterprise Author 是德国思爱普（SAP）公司的一个用于管理 2D、3D、动画、视频和音频资产的桌面应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取 HTTP 请求中的敏感信息，发送具有不同方法类型的多个 Http 请求，导致拒绝服务等。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS for Java 拒绝服务漏洞、SAP NetWeaver AS JAVA 信息泄露漏洞（CNVD-2022-69287）、SAP 3D Visual Enterprise Author 缓冲区溢出漏洞（CNVD-2022-69691、CNVD-2022-69694、CNVD-2022-69693、CNVD-2022-69692、CNVD-2022-69697、CNVD-2022-69696）。其中，“SAP 3D Visual Enterprise Author 缓冲区溢出漏洞（CNVD-2022-69691、CNVD-2022-69693）”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-2022-69288

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69287

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69691

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69694

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69693

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69692

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69697

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69696

2、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。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，获得系统上的提升权限等。

CNVD 收录的相关漏洞包括：Linux kernel 资源管理错误漏洞（CNVD-2022-69188、CNVD-2022-69187、CNVD-2022-69186、CNVD-2022-69189、CNVD-2022-69192、CNVD-2022-69191）、Linux kernel 权限提升漏洞（CNVD-2022-69197、CNVD-2022-69204）。其中，“Linux kernel 权限提升漏洞（CNVD-2022-69197、CNVD-2022-69204）”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-2022-69188

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69187

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69186

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69189

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69192

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69191

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69197

https://www.cnvd.org.cn/flaw/show/CNVD-2022-69204

3、Apache 产品安全漏洞

Apache Pulsar 是美国阿帕奇（Apache）基金会的一个用于云环境种，集消息、存储、轻量化函数式计算为一体的分布式消息流平台。该软件支持多租户、持久化存储、多机房跨区域数据复制，具有强一致性、高吞吐以及低延时的高可扩展流数据存储特性。Apache IoTDB 是美国阿帕奇（Apache）基金会的一款为时间序列数据设计的集成数据管理引擎，它能够提供数据收集、存储和分析服务等。Apache Tapestry 是美国阿帕奇（Apache）基金会的一款使用 Java 语言编写的 Web 应用程序框架。Apache Dubbo 是一款微服务开发框架，它提供了 RPC 通信与微服务治理两大关键能力。Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持。Apache Jetspeed-2 是美国阿帕奇（Apache）基金会的一个非常开放和可定制的门户平台。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 Proxy 实现中间人攻击，绕过身份验证过程并在特定情况下接管其他 Web 应用程序用户的帐户，导致拒绝服务(ReDoS)攻击等。

CNVD 收录的相关漏洞包括：Apache Pulsar 信任管理问题漏洞（CNVD-2022-69470、CNVD-2022-69468）、Apache IoTDB 访问控制错误漏洞、Apache IoTDB 授权问题漏洞（CNVD-2022-69472）、Apache Tapestry 拒绝服务漏洞（CNVD-2022-69475）、A

pache Dubbo Hession 反序列化漏洞、Apache Tomcat 请求混淆漏洞、Apache Jetspeed-2 输入验证错误漏洞。其中，除“Apache Pulsar 信任管理问题漏洞（CNVD-2022-69470、CNVD-2022-69468）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-2022-69470
https://www.cnvd.org.cn/flaw/show/CNVD-2022-69468
https://www.cnvd.org.cn/flaw/show/CNVD-2022-69473
https://www.cnvd.org.cn/flaw/show/CNVD-2022-69472
https://www.cnvd.org.cn/flaw/show/CNVD-2022-69475
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70071
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70612
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70611

4、Microsoft 产品安全漏洞

Microsoft Windows Print Spooler Components 是美国微软（Microsoft）公司的一个打印后台处理程序组件。Microsoft Windows Remote Access Connection Manager 是美国微软（Microsoft）公司的一项 Windows 服务，用于管理从您的计算机到 Internet 的虚拟专用网络 (VPN)连接，如果禁用此服务，VPN 客户端应用程序将无法启动。Microsoft Windows Push Notifications 是美国微软（Microsoft）公司的一个推送通知服务。它提供了一种可靠的方式提供新的更新。Microsoft Windows Storage Spaces Controller 是美国微软（Microsoft）公司的提供存储空间功能的必要驱动程序。Microsoft Windows 是美国微软（Microsoft）公司的一种桌面操作系统。Microsoft Windows Remote Procedure Call Runtime 是美国微软（Microsoft）公司的一种用于创建分布式客户端/服务器程序的技术。Microsoft Windows Remote Desktop Protocol（RDP）是美国微软（Microsoft）公司的一款用于连接远程 Windows 桌面的应用。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，导致任意代码执行或权限提升等。

CNVD 收录的相关漏洞包括：Microsoft Windows Print Spooler Components 权限提升漏洞（CNVD-2022-70056）、Microsoft Windows Remote Access Connection Manager 权限提升漏洞（CNVD-2022-70059）、Microsoft Windows Push Notifications 权限提升漏洞、Microsoft Windows Storage Spaces Controller 权限提升漏洞（CNVD-2022-70064、CNVD-2022-70065）、Microsoft Windows Server Service 信息泄露漏洞、Microsoft Windows Remote Procedure Call Runtime 远程代码执行漏洞、Microsoft Windows Remote Desktop Protocol 信息泄露漏洞（CNVD-2022-70061）。其中，“Microsoft Windows Print Spooler Components 权限提升漏洞（CNVD-2022-70056）、Microsoft Windows Storage Spaces Controller 权限提升漏洞（CNVD-2022-70065）”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-2022-70056
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70059
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70058
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70064
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70063
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70062
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70061
https://www.cnvd.org.cn/flaw/show/CNVD-2022-70065

5、Schneider Electric Easergy P5 缓冲区溢出漏洞

Schneider Electric Easergy P5 是法国施耐德电气（Schneider Electric）公司的一款适用于要求苛刻的中压应用的保护继电器。本周，Schneider Electric Easergy P5 被披露存在缓冲区溢出漏洞。攻击者可以利用该漏洞在系统上执行任意代码。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-2022-70104

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-2022-69695	SAP 3D Visual Enterprise Author 缓冲区溢出漏洞（CNVD-2022-69695）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://launchpad.support.sap.com/#/notes/3245929
CNVD-2022-70025	Apache Airflow 代码问题漏洞	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.apache.org/thread/ohf3pvd3dftb8zb01yngbn1jtkq5m08y
CNVD-2022-70582	FFmpeg 缓冲区溢出漏洞（CNVD-2022-70582）	高	目前厂商已经发布了升级补丁以修复这个问题，请到厂商的主页下载：https://github.com/FFmpeg/FFmpeg/commit/c953baa084607dd1d84c3bfcce3cf6a87c3e6e05
CNVD-2022-70585	WhatsApp 数字错误漏洞	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.whatsapp.com/security/advisories/2022/
CNVD-2022	Rocket.Chat 授权问题漏洞（C	高	目前厂商已发布升级补丁以修复漏

-70584	NVD-2022-70584）		洞，详情请关注厂商主页：https://www.rocket.chat
CNVD-2022-70597	Home Owners Collection Management System SQL 注入漏洞（CNVD-2022-70597）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcecodester.com/php/15162/home-owners-collection-management-system-phpoop-free-source-code.html
CNVD-2022-69723	TOTOLINK T8 存在缓冲区溢出漏洞（CNVD-2022-69723）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=18&ids=33
CNVD-2022-69735	Samsung AppLinker 隐式意图劫持漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7
CNVD-2022-69204	Linux kernel 权限提升漏洞（CNVD-2022-69204）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb
CNVD-2022-69197	Linux kernel 权限提升漏洞（CNVD-2022-69197）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://bugzilla.redhat.com/show_bug.cgi?id=2027201

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 HTTP 请求中的敏感信息，发送具有不同方法类型的多个 Http 请求，导致拒绝服务等。此外，Linux、Apache、Microsoft 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，任意代码执行，通过 Proxy 实现中间人攻击，绕过身份验证过程并在特定情况下接管其他 Web 应用程序用户的帐户，导致拒绝服务(ReDoS)攻击等。另外，Schneider Electric Easergy P5 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞在系统上执行任意代码。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、Wedding Planner select.php SQL 注入漏洞

验证描述

Wedding Planner 是一个婚礼策划师项目。旨在为用户提供一种简单的方法，让他们在使用真实数据的同时通过 Web 应用程序来计划他们的婚礼。

Wedding Planner v1.0 版本存在 SQL 注入漏洞，该漏洞源于/admin/select.php 中的 id 参数缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/jayus0821/uai-poc/blob/main/Netgear/WNAP320/unauth.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-70026

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. 数千 GitHub 存储库提供带有恶意软件的假 PoC 漏洞

莱顿高级计算机科学研究所的研究人员在 GitHub 上发现了数以千计的存储库，为各种漏洞提供虚假的概念验证（PoC）利用，其中一些包括恶意软件。

参考链接：https://www.bleepingcomputer.com/news/security/thousands-of-github-repositories-deliver-fake-poc-exploits-with-malware/

2. 微软确认 Outlook 存在问题导致 Exchange Online 邮箱无法配置

微软发布支持文档，确认了 Outlook 中的一个新 Bug。据悉，该 Bug 可能导致用户尝试使用 Outlook 与 Exchange Online 邮箱连接时失败，并提示错误代码 603“无法配置 Exchange Online 邮箱”。

参考链接：https://www.cnbeta.com/articles/tech/1330145.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