国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 04 月 29 日-2024 年 05 月 12 日

2024 年第 18、19 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 605 个，其中高危漏洞 247 个、中危漏洞 339 个、低危漏洞 19 个。漏洞平均分值为 6.32。本周收录的漏洞中，涉及 0day 漏洞 480 个（占 79%），其中互联网上出现“Tenda AC 10U setSmartPowerManagement 函数堆栈缓冲区溢出漏洞、libming parseSWF_TEXTRECORD 功能内存泄露漏洞”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 14234 个，与上周（7766 个）环比增加 83%。

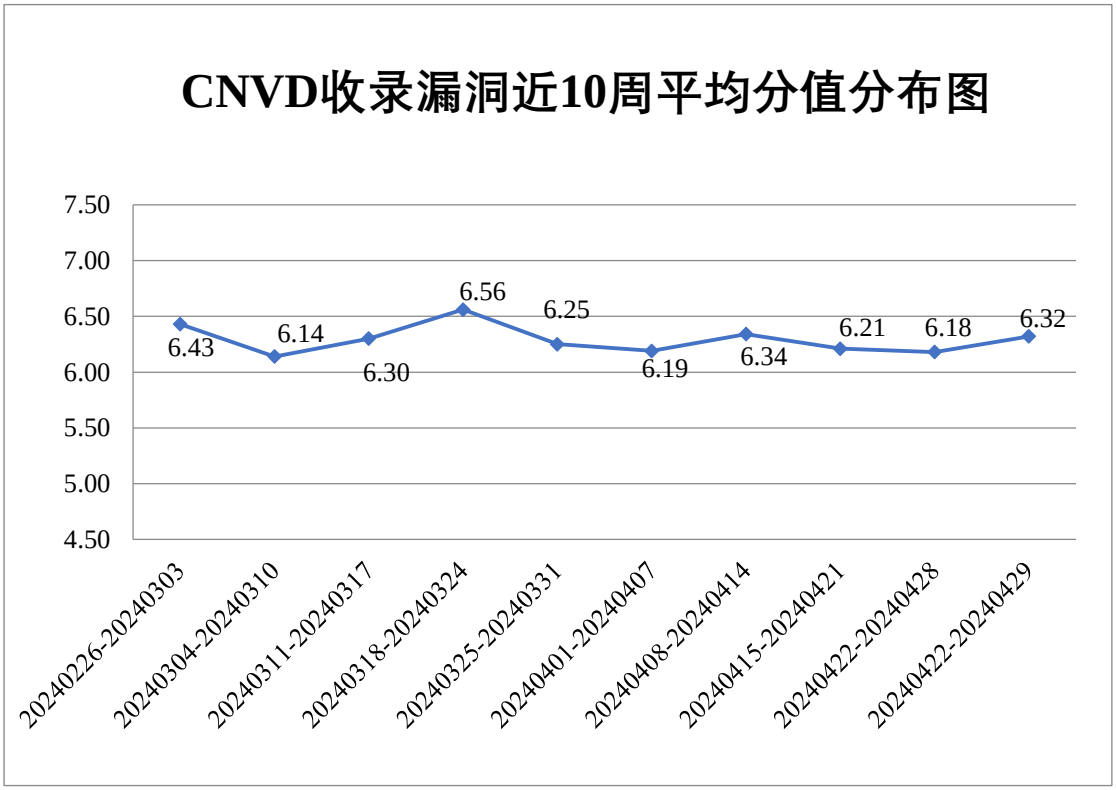

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 起，向基础电信企业通报漏洞事件 5 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 822 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 111 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 37 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、重庆衡泽软件科技有限公司、中网智达（河北）网络科技有限公司、中科博华信息科技有限公司、中保科技集團、浙江智游宝信息科技有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、雅马哈乐器音响（中国）投资有限公司、兄弟（中国）商业有限公司、信呼、新天科技股份有限公司、新都(青岛)电子有限公司、祥云县上云六零科技工作室、西安众邦网络科技有限公司、西安瑞友信息技术资讯有限公司、西安交大捷普网络科技有限公司、武汉三佳医疗信息技术有限公司、无锡金软科技有限公司、微软（中国）有限公司、网件（北京）网络技术有限公司、万洲电气股份有限公司、同望科技股份有限公司、天翼云科技有限公司、世邦通信股份有限公司、沈阳泰科易科技有限公司、神州数码控股有限公司、神州数码集团股份有限公司、深圳维盟网络技术有限公司、深圳维盟科技股份有限公司、深圳图邦软件信息技术有限公司、深圳拓安信物联股份有限公司、深圳市中电电力技术股份有限公司、深圳市优卡特电子有限公司、深圳市迅捷通信技术有限公司、深圳市唯传科技有限公司、深圳市微耕实业有限公司、深圳市思迪信息技术股份有限公司、深圳市三联众瑞科技有限公司、深圳市赛格导航科技股份有限公司、深圳市锐明技术股份有限公司、深圳市美科星通信技术有限公司、深圳市蓝拓创远科技有限公司、深圳市蓝凌软件股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市红门智慧停车科技有限公司、深圳市冠卓科技有限公司、深圳市电速科技有限公司、深圳市道尔智控科技股份有限公司、深圳市步科电气有限公司、深圳市博实结科技股份有限公司、深圳市百为通达科技有限公司、深圳锐取信息技术股份有限公司、深圳华视美达信息技术有限公司、深圳彼度科技有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海桑锐电子科技股份有限公司、上海三高计算机中心股份有限公司、上海瑞策软件有限公司、上海肯特仪表股份有限公司、上海居亦科技发展有限公司、上海华测导航技术股份有限公司、上海格瑞特科技实业股份有限公司、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、上海伯俊软件科技有限公司、商派软件有限公司、山东潍微科技股份有限公司、厦门网中网软件有限公司、厦门天锐科技股份有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、融智通科技（北京）股份有限公司、青岛三利集团有限公司、青岛和正信息技术有限公司、青岛海威茨

仪表有限公司、麒麟软件有限公司、普元信息技术股份有限公司、普联技术有限公司、南京星远图科技有限公司、南京昆石网络技术有限公司、南京科远智慧科技集团股份有限公司、南昌蓝智科技有限公司、南昌航天广信科技有限责任公司、领航未来（北京）科技有限公司、联奕科技股份有限公司、联想集团、朗坤智慧科技股份有限公司、蓝网科技股份有限公司、兰吉尔仪表系统（珠海）有限公司、科众三六五科技有限公司、柯尼卡美能达集团、京师心智（北京）科技服务有限公司、京瓷办公信息系统（中国）有限公司、锦岸机械科技江苏有限公司、江苏三恒科技股份有限公司、江苏赛达电子科技有限公司、江苏麦维智能科技有限公司、佳能（中国）有限公司、济南瑞泉电子有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南科创信息技术股份有限公司、湖南建研信息技术股份有限公司、湖北点点点科技有限公司、河北先河环保科技股份有限公司、河北汉联信息科技有限公司、杭州云润科技有限公司、杭州海康威视数字技术股份有限公司、杭州当虹科技股份有限公司、国药控股江苏有限公司、广州易凯软件技术有限公司、广州图创计算机软件开发有限公司、广州市中大东日教育技术有限公司、广州市保伦电子有限公司、广州红海云计算股份有限公司、广州澳视德软件科技有限公司、广东飞企互联科技股份有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、福建星网锐捷通讯股份有限公司、福建科立讯通信有限公司、福建汇川物联网技术科技股份有限公司、东方网力科技股份有限公司、帝国软件、大唐高鸿信息技术有限公司、大汉软件股份有限公司、成都虚谷伟业科技有限公司、成都添闰通讯技术有限公司、成都市任我行信息技术有限公司、成都华栖云科技有限公司、畅捷通信息技术股份有限公司、常州新阳科技服务有限公司、北京中农信达信息技术有限公司、北京智芯微电子科技有限公司、北京致远互联软件股份有限公司、北京易联易通科技有限公司、北京亿信华辰软件有限责任公司、北京亿赛通科技发展有限责任公司、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、北京万户软件技术有限公司、北京硕人时代科技股份有限公司、北京神州视翰科技有限公司、北京三快科技有限公司、北京润乾信息系统技术有限公司、北京敲敲云科技有限公司、北京平凯星辰科技发展有限公司、北京派可数据科技有限公司、北京美特软件技术有限公司、北京久其软件股份有限公司、北京金山办公软件股份有限公司、北京金和网络股份有限公司、北京火木科技有限公司、北京豆网科技有限公司、北京超图软件股份有限公司、北京北信源软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、安移通网络科技（中国）有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、爱普生（中国）有限公司、Seacms 和 ABB。

本周，CNVD 发布了《F5 发布 2024 年 5 月季度安全通告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9991

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、北京天融信网络安全技术有限公司、阿里云计算有限公司、北京数字观星科技有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。江苏金盾检测技术股份有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、成都久信信息技术股份有限公司、联想集团、西藏熙安信息技术有限责任公司、安徽天行网安信息安全技术有限公司、北京山石网科信息技术有限公司、江苏晟晖信息科技有限公司、中资网络信息安全科技有限公司、苏州棱镜七彩信息科技有限公司、内蒙古中叶信息技术有限责任公司、河南灵创电子科技有限公司、江苏锋刃信息科技有限公司、北京中睿天下信息技术有限公司、内蒙古洞明科技有限公司、广州安亿信软件科技有限公司、中国电信股份有限公司上海研究院、西藏闪锁网络科技有限公司、重庆都会信息科技有限公司、北京天防安全科技有限公司、江苏天创科技有限公司、山东云天安全技术有限公司、湖南泛联新安信息科技有限公司、国网山东省电力公司、山石网科通信技术股份有限公司、成都安美勤信息技术股份有限公司、陕西青山四纪信息技术有限公司、联通数字科技有限公司、江苏极元信息技术有限公司、北京微步在线科技有限公司、成都思维世纪科技有限责任公司、安徽长泰科技有限公司、博智安全科技股份有限公司、中国工程物理研究院计算机应用研究所、杭州中正检测技术有限公司、北京中关村实验室、工业和信息化部电子第五研究所-数据治理服务中心、江苏省公用信息有限公司、北京时代新威信息技术有限公司、上海观安信息技术股份有限公司、浙江东安检测技术有限公司、中华人民共和国山东海事局、国家能源集团、江西中和证信息安全技术有限公司、新疆海狼科技有限公司、上海亿保健康科技集团有限公司、浙江大学控制科学与工程学院及其他个人白帽子向 CNVD 提交了 14234 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 12086 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	原创漏洞数量
斗象科技（漏洞盒子）	6359	6359
奇安信网神（补天平台）	3872	3872
上海交大	1473	1473
新华三技术有限公司	1175	0
三六零数字安全科技集团有限公司	382	382

北京天融信网络安全技术有限公司	295	34
阿里云计算有限公司	261	0
北京数字观星科技有限公司	254	0
华为技术有限公司	160	1
恒安嘉新（北京）科技股份公司	95	0
北京启明星辰信息安全技术有限公司	68	1
北京知道创宇信息技术有限公司	62	0
北京安信天行科技有限公司	41	41
北京升鑫网络科技有限公司（青藤云）	39	39
中国电信集团系统集成有限责任公司	21	0
远江盛邦（北京）网络安全科技股份有限公司	19	19
北京长亭科技有限公司	11	9
杭州迪普科技股份有限公司	10	0
北京智游网安科技有限公司	4	4
江苏金盾检测技术股份有限公司	130	130
快页信息技术有限公司	55	55
河南东方云盾信息技术有限公司	52	52
成都久信信息技术股份有限公司	28	28

联想集团	25	25
西藏熙安信息技术有限责任公司	25	25
安徽天行网安信息安全技术有限公司	13	13
北京山石网科信息技术有限公司	11	11
江苏晟晖信息科技有限公司	8	8
中资网络信息安全科技有限公司	8	8
苏州棱镜七彩信息科技有限公司	7	7
内蒙古中叶信息技术有限责任公司	7	7
河南灵创电子科技有限公司	7	7
江苏锋刃信息科技有限公司	5	5
北京中睿天下信息技术有限公司	5	5
内蒙古洞明科技有限公司	5	5
广州安亿信软件科技有限公司	4	4
中国电信股份有限公司上海研究院	4	4
西藏闪锁网络科技有限公司	4	4
重庆都会信息科技有限公司	3	3
北京天防安全科技有限公司	3	3
江苏天创科技有限公司	3	3

山东云天安全技术有限公司	3	3
湖南泛联新安信息科技有限公司	3	3
国网山东省电力公司	3	3
山石网科通信技术股份有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
陕西青山四纪信息技术有限公司	2	2
联通数字科技有限公司	2	2
江苏极元信息技术有限公司	2	2
北京微步在线科技有限公司	2	2
成都思维世纪科技有限责任公司	2	2
安徽长泰科技有限公司	1	1
博智安全科技股份有限公司	1	1
中国工程物理研究院计算机应用研究所	1	1
杭州中正检测技术有限公司	1	1
北京中关村实验室	1	1
工业和信息化部电子第五研究所-数据治理服务中心	1	1
江苏省公用信息有限公司	1	1
北京时代新威信息技术有限公司	1	1

上海观安信息技术股份有限公司	1	1
浙江东安检测技术有限公司	1	1
中华人民共和国山东海事局	1	1
国家能源集团	1	1
江西中和证信息安全技术有限公司	1	1
新疆海狼科技有限公司	1	1
上海亿保健康科技集团有限公司	1	1
浙江大学控制科学与工程学院	1	1
CNCERT 宁夏分中心	22	22
CNCERT 贵州分中心	4	4
个人	1523	1523
报送总计	16601	14234

本周漏洞按类型和厂商统计

本周，CNVD 收录了 605 个漏洞。WEB 应用 273 个，应用程序 161 个，网络设备（交换机、路由器等网络端设备）77 个，智能设备（物联网终端设备）44 个，数据库 25 个，操作系统 17 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	273
应用程序	161
网络设备（交换机、路由器等网络端设备）	77
智能设备（物联网终端设备）	44
数据库	25
操作系统	17
安全产品	8

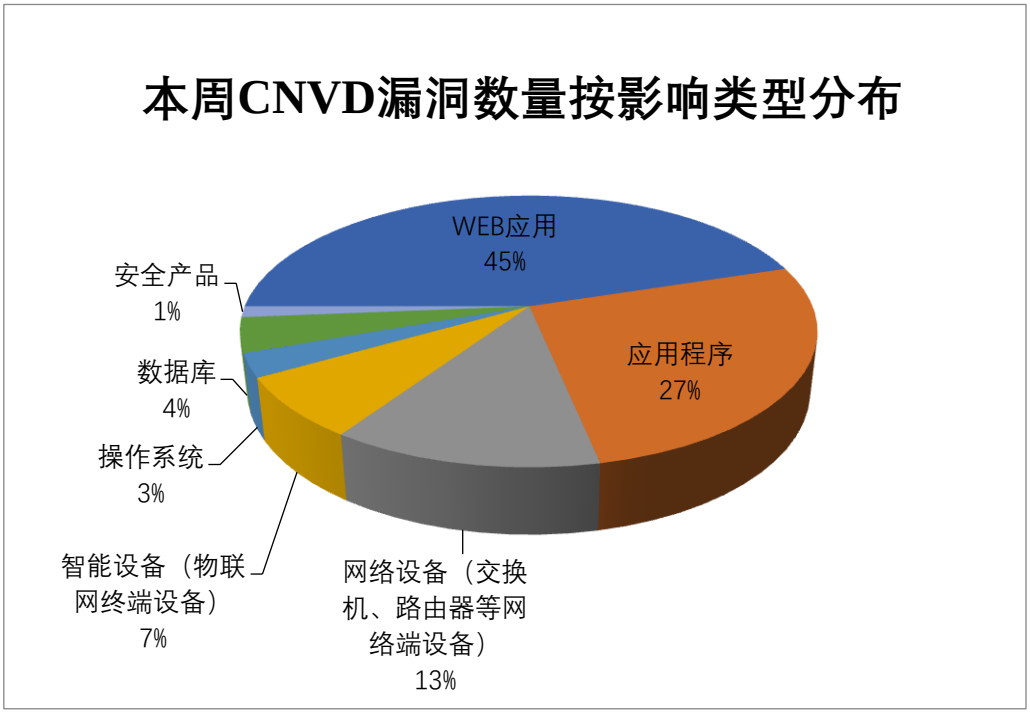

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Oracle、用友网络科技股份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	Adobe	24	4%
2	Oracle	18	3%
3	用友网络科技股份有限公司	14	2%
4	北京百卓网络技术有限公司	13	2%
5	F5	13	2%
6	Microsoft	12	2%
7	Apache	11	2%
8	北京星网锐捷网络技术有限公司	10	2%
9	Cisco	10	2%
10	其他	480	79%

本周行业漏洞收录情况

本周，CNVD 收录了 47 个电信行业漏洞，45 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，“Oracle MySQL 拒绝服务漏洞（CNVD-2024-20817）、

Google Android 权限提升漏洞（CNVD-2024-21190）”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/

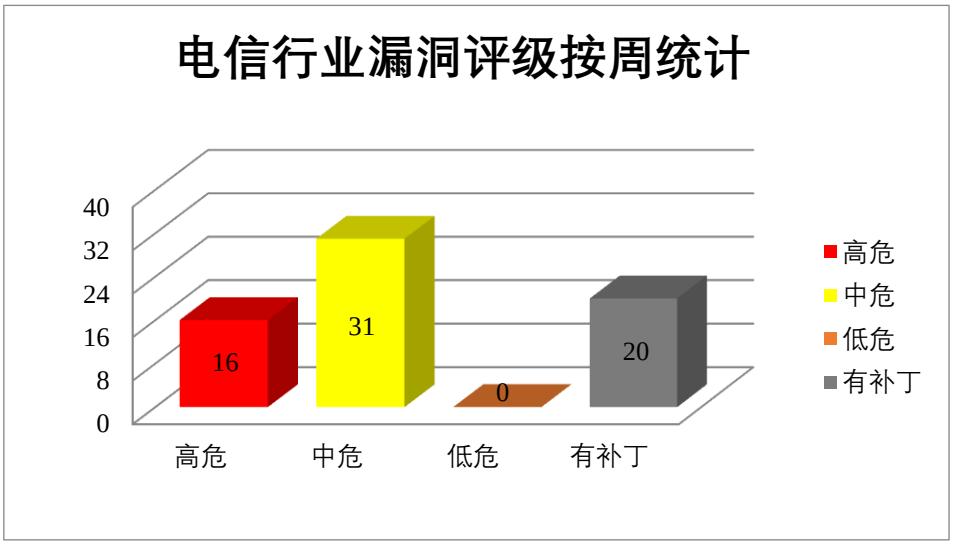

图 3 电信行业漏洞统计

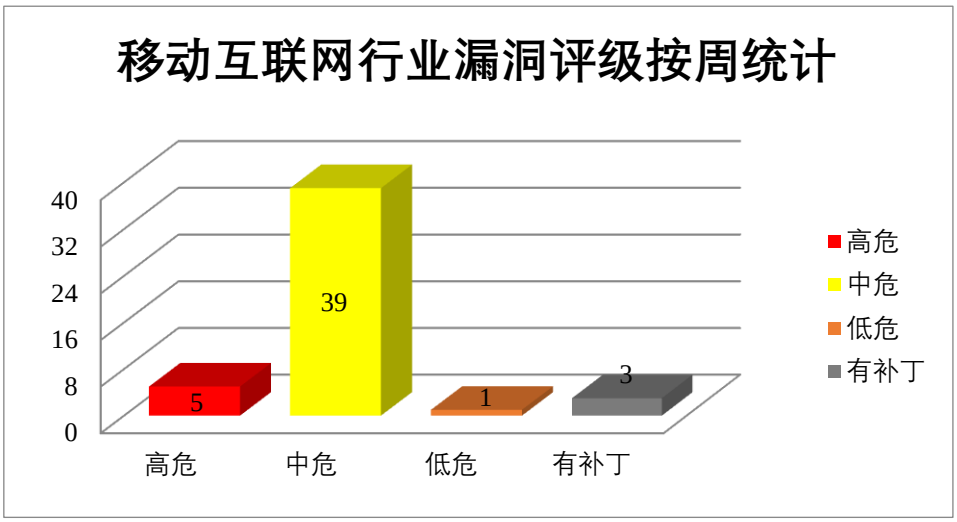

图 4 移动互联网行业漏洞统计

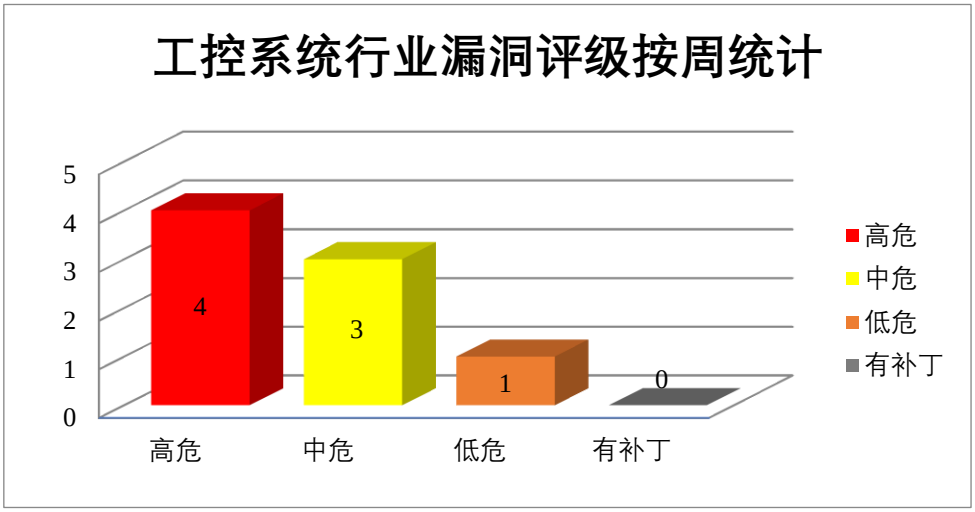

图 5 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、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 CloudStack 是美国阿帕奇（Apache）基金会的一套基础架构即服务（IaaS）云计算平台。该平台主要用于部署和管理大型虚拟机网络。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 HugeGraph 是美国阿帕奇（Apache）基金会的一个速度快、可扩展性强的图形数据库。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过保护机制，通过配置 UI 页面查看敏感信息，在系统上执行任意命令，导致内存耗尽等。

CNVD 收录的相关漏洞包括：Apache HugeGraph-Server 命令执行漏洞、Apache HugeGraph-Server 安全绕过漏洞、Apache HugeGraph-Hubble 服务器端请求伪造漏洞、Apache Airflow FTP Provider 信任管理问题漏洞、Apache Airflow 信息泄露漏洞（CNVD-2024-20804）、Apache CloudStack 输入验证错误漏洞（CNVD-2024-20836）、Apache CloudStack 安全绕过漏洞、Apache HTTP Server 资源管理错误漏洞。其中，除“Apache Airflow 信息泄露漏洞（CNVD-2024-20804）”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-2024-20803

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20802

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20801

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20800

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20804

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20836

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20838

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20839

2、 Microsoft 产品安全漏洞

Microsoft Windows USB Hub Driver 是美国微软（Microsoft）公司的一个驱动程序。Microsoft Windows Kernel 是美国微软（Microsoft）公司的 Windows 操作系统的内核。Microsoft Windows Kerberos 是美国微软（Microsoft）公司的一个用于在网络集群中进行身份验证的软件。Kerberos 同时作为一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供认证服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过某些功能，获取敏感信息，提升权限，在系统上执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Windows USB Hub Driver 远程代码执行漏洞、Microsoft Windows Kernel 拒绝服务漏洞、Microsoft Windows Kernel 权限提升漏洞（CNVD-2024-21146、CNVD-2024-21148、CNVD-2024-21151）、Microsoft Windows Kernel 信息泄露漏洞（CNVD-2024-21149、CNVD-2024-21150）、Microsoft Windows Kerberos 安全功能绕过漏洞。其中，“Microsoft Windows USB Hub Driver 远程代码执行漏洞、Microsoft Windows Kerberos 安全功能绕过漏洞”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-2024-21143

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21145

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21146

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21148

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21149

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21150

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21151

https://www.cnvd.org.cn/flaw/show/CNVD-2024-21152

3、 Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞导致 MySQL 服务器挂起或频繁重复崩溃。

CNVD 收录的相关漏洞包括：Oracle MySQL 拒绝服务漏洞（CNVD-2024-20806、CNVD-2024-20805、CNVD-2024-20809、CNVD-2024-20808、CNVD-2024-20807、CNV

D-2024-20813、CNVD-2024-20812、CNVD-2024-20811）。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-2024-20806
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20805
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20809
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20808
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20807
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20813
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20812
https://www.cnvd.org.cn/flaw/show/CNVD-2024-20811

4、Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。Adobe InDesign 是美国奥多比（Adobe）公司的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，攻击者可利用漏洞绕过安全措施，获得对敏感文件的未经授权的访问权限，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 Bridge 堆缓冲区溢出漏洞（CNVD-2024-21153）、Adobe Bridge 越界写入漏洞（CNVD-2024-21154）、Adobe Bridge 内存错误引用漏洞（CNVD-2024-21155）、Adobe ColdFusion 访问控制错误漏洞（CNVD-2024-21156）、Adobe InDesign 越界读取漏洞（CNVD-2024-21162、CNVD-2024-21165）、Adobe Premiere Pro 堆缓冲区溢出漏洞、Adobe Premiere Pro 越界写入漏洞。其中，除“Adobe InDesign 越界读取漏洞（CNVD-2024-21162、CNVD-2024-21165）”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-2024-21153
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21154
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21155
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21156
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21162
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21165
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21670
https://www.cnvd.org.cn/flaw/show/CNVD-2024-21671

5、TOTOLINK EX1800T langType 参数命令执行漏洞

TOTOLINK EX1800T 是中国吉翁电子（TOTOLINK）公司的一款 Wi-Fi 范围扩展

器。本周，TOTOLINK EX1800T 被披露存在命令执行漏洞。攻击者可利用该漏洞在系统上执行任意命令。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-2024-21655

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-2024-20821	IBM Security Verify Access 信任管理问题漏洞（CNVD-2024-20821）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7147932
CNVD-2024-20840	IBM Personal Communications 任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://exchange.xforce.ibmcloud.com/vulnerabilities/281619
CNVD-2024-21191	Google Android 权限提升漏洞（CNVD-2024-21191）	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/2023-02-01
CNVD-2024-21210	Ivanti Avalanche 堆溢出漏洞	高	厂商已发布了修复漏洞的新版本，请及时关注更新：https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US
CNVD-2024-21219	Delta Electronics DIAEnergie Handler_CFG.ashx 脚本 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://www.deltaww.com/
CNVD-2024-21266	Fortinet FortiSandbox 路径遍历漏洞（CNVD-2024-21266）	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：https://www.fortiguard.com/psirt/FG-IR-23-454
CNVD-2024-21665	Tinyproxy HTTP 头处理内存错误引用漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/tinyproxy/tinyproxy
CNVD-2024-22208	F5 BIG-IP AFM 拒绝服务漏洞（CNVD-2024-22208）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K000139037
CNVD-2024	F5 BIG-IP Next Central Ma	高	厂商已发布了漏洞修复程序，请及

-22209	nager SQL 注入漏洞		时关注更新：https://my.f5.com/manage/s/article/K000138733
CNVD-2024-22210	F5 BIG-IP Next Central Manager OData 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://my.f5.com/manage/s/article/K000138732

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用漏洞绕过保护机制，通过配置 UI 页面查看敏感信息，在系统上执行任意命令，导致内存耗尽等。此外，Microsoft、Oracle、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过某些功能，获取敏感信息，提升权限，在当前用户的上下文中执行任意代码，造成拒绝服务等。另外，TOTOLINK EX1800T 被披露存在命令执行漏洞。攻击者可利用该漏洞在系统上执行任意命令。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、Tenda AC10U setSmartPowerManagement 函数堆栈缓冲区溢出漏洞

验证描述

Tenda AC10U 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10U setSmartPowerManagement 函数存在堆栈缓冲区溢出漏洞，该漏洞是由于 setSmartPowerManagement 函数未能正确边界检查引起的。攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码。

验证信息

POC 链接：https://github.com/yaoyue123/iot/blob/main/Tenda/AC10U/setSmartPowerManagement.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-21489

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. TunnelVision 漏洞曝光，几乎可监听所有 VPN

近日，安全企业 Leviathan Security Group 披露了一个名为 TunnelVision 的安全漏洞，它可将用户的 VPN 流量外泄给位于同一局域网络上的黑客，该漏洞被追踪为 CVE-2024-3661。

参考链接：https://www.freebuf.com/news/400347.html

2. F5 管理器存在安全漏洞，能让攻击者开设账户并长期潜伏

据供应链网络安全公司 Eclypsium 5 月 8 日发布的一份报告，研究人员在 F5 的 Next Central Manager 中发现了安全漏洞，可使攻击者长期且隐蔽地存在于任何 F5 资产相关的组织网络基础设施中。

参考链接：https://www.freebuf.com/news/400364.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