国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 11 月 25 日-2024 年 12 月 01 日　　2024 年第 48 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 445 个，其中高危漏洞 208 个、中危漏洞 212 个、低危漏洞 25 个。漏洞平均分值为 6.52。本周收录的漏洞中，涉及 0day 漏洞 261 个（占 59%），其中互联网上出现“D-Link DWR-2000M 跨站脚本漏洞、TP-LINK TL-WDR7660 缓冲区溢出漏洞”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 3972 个，与上周（3062 个）环比增加 30%。

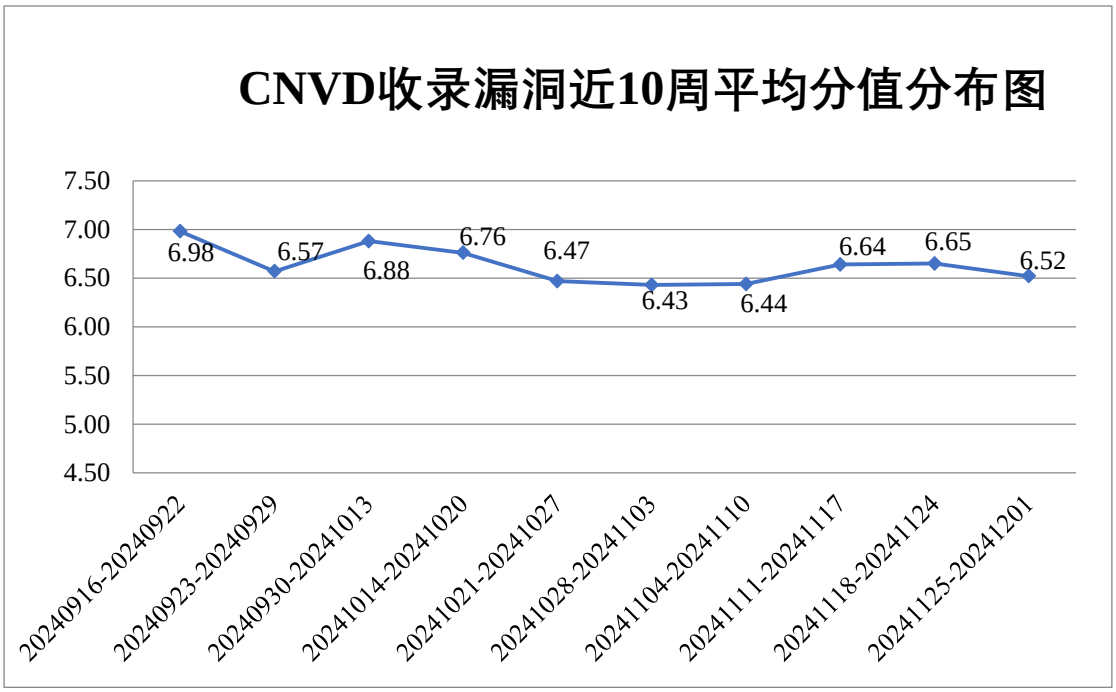

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 572 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 84 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 17 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：

卓豪（中国）技术有限公司、珠海市安克电子技术有限公司、重庆攀宝科技有限公司、中控技术股份有限公司、中科数字通（北京）科技有限公司、中科方德软件有限公司、智互联（深圳）科技有限公司、智恒科技股份有限公司、郑州市金水区恒友摄影软件经营部、郑州华粮科技股份有限公司、正元智慧集团股份有限公司、正方软件股份有限公司、浙江宇视科技有限公司、长春吉大正元信息技术股份有限公司、云南奇讯科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、新道科技股份有限公司、西门子（中国）有限公司、武汉中云康崇科技有限公司、武汉三佳医疗信息技术有限公司、武汉达梦数据库股份有限公司、无锡信捷电气股份有限公司、卫宁健康科技集团股份有限公司、万洲电气股份有限公司、万可电子（天津）有限公司、腾讯安全应急响应中心、台达电子企业管理（上海）有限公司、四川迅睿云软件开发有限公司、四川天健世纪科技有限公司、深圳拓安信物联股份有限公司、深圳市优软科技有限公司、深圳市亿玛信诺科技有限公司、深圳市同享软件科技有限公司、深圳市思迅软件股份有限公司、深圳市深科特信息技术有限公司、深圳市锐明技术股份有限公司、深圳市明源云科技有限公司、深圳市联软科技股份有限公司、深圳市磊科实业有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市大疆创新科技有限公司、深圳市宝创科技有限公司、深圳市爱德数智科技股份有限公司、深圳勤杰软件有限公司、深圳齐心好视通云计算有限公司、深圳华颐智能系统有限公司、深圳国威电子有限公司、上海卓卓网络科技有限公司、上海正品贵德软件有限公司、上海甄云科技信息有限公司、上海易立德信息技术股份有限公司、上海商创网络科技有限公司、上海三高计算机中心股份有限公司、上海穆云智能科技有限公司、上海肯特仪表股份有限公司、上海金慧软件有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海电音马兰士电子有限公司、上海点都数字科技有限公司、上海贝锐信息科技股份有限公司、上海艾泰科技有限公司、三星（中国）投资有限公司、三未信安科技股份有限公司、青果软件集团有限公司、青岛鼎信通讯股份有限公司、麒麟软件有限公司、普联技术有限公司、诺梵（上海）系统科技股份有限公司、南京联衡电子有限公司、南京金鹊软件科技有限公司、南京博纳睿通软件科技有限公司、南昌卓蓝科技有限公司、领航未来（北京）科技有限公司、联奕科技股份有限公司、朗坤智慧科技股份有限公司、柯尼卡美能达集团、佳能（中国）有限公司、吉翁电子（深圳）有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南众合百易信息技术有限公司、杭州连边科技有限公司、杭州海康威视数字技术股份有限公司、

杭州飞致云信息科技有限公司、杭州安恒信息技术股份有限公司、国泰新点软件股份有限公司、贵州小码科技有限公司、广州易凯软件技术有限公司、广州讯尔软件科技有限公司、广州市保伦电子有限公司、广州热点软件科技股份有限公司、广州蓝鸽科技有限公司、广州红海云计算股份有限公司、广州恒企教育科技有限公司、广州非凡信息安全技术有限公司、广州博控自动化技术有限公司、广东中兴新支点技术有限公司、广东中设智控科技股份有限公司、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、固德威技术股份有限公司、富士施乐（中国）有限公司、富士胶片商业创新（中国）有限公司、福建银达汇智信息科技股份有限公司、福建星网智慧科技有限公司、戴尔(中国)有限公司、成都汇聚达软件有限公司、畅捷通信息技术股份有限公司、北京云因信息技术有限公司、北京优锘科技有限公司、北京易普行科技有限公司、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、北京信诺瑞得软件系统有限公司、北京小桔科技有限公司、北京万户软件技术有限公司、北京统御至诚科技有限公司、北京通达信科科技有限公司、北京世纪超星信息技术发展有限责任公司、北京神州数码云计算有限公司、北京神州视翰科技有限公司、北京美特软件技术有限公司、北京龙软科技股份有限公司、北京雷石天地电子技术有限公司、北京莱特林客光电技术有限公司、北京金和网络股份有限公司、北京慧舟普度科技有限公司、北京弘文恒瑞文化传播有限公司、北京德信远医药科技发展有限公司、北京安信天行科技有限公司、北京安信立融科技股份有限公司、百度安全应急响应中心、安科瑞电气股份有限公司、安徽商信政通信息技术股份有限公司、安徽科迅教育装备集团有限公司、爱普生（中国）有限公司、ONKYO 安桥安桥（上海）商贸有限公司和《中国学术期刊（光盘版）》电子杂志社有限公司。

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、北京神州绿盟科技有限公司、新华三技术有限公司、北京数字观星科技有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、河南东方云盾信息技术有限公司、中孚安全技术有限公司、北京翰慧投资咨询有限公司、苏州棱镜七彩信息科技有限公司、淮安易云科技有限公司、贵州多彩网安科技有限公司、联通数字科技有限公司、北京纽盾网安信息技术有限公司、北京山石网科信息技术有限公司、江苏云天网络安全技术有限公司、江苏保旺达软件技术有限公司、上海维信荟智金融科技有限公司、成都安美勤信息技术股份有限公司、北京安帝科技有限公司、平安银河实验室、信息产业信息安全测评中心、中资网络信息安全科技有限公司、深圳昂楷科技有限公司、北京时代新威信息技术有限公司、北京君云天下科技有限公司、江苏金盾检测技术股份有限公司、中国工商银行、上海亿保健康科技集团有限公司、中国银行、

江苏耘和计算机系统工程有限公司、超聚变数字技术有限公司、陕西青山四纪信息技术有限公司、江苏正信信息安全测试有限公司、上海吨吨信息技术有限公司、国网江西省电力有限公司电力科学研究院、武汉绿色网络股份有限责任公司、国家计算机病毒应急处理中心及其他个人白帽子向 CNVD 提交了 3972 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）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 2476 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
深信服科技股份有限公司	2116	9
斗象科技（漏洞盒子）	1781	1781
北京神州绿盟科技有限公司	1155	120
新华三技术有限公司	688	0
北京数字观星科技有限公司	673	0
北京天融信网络安全技术有限公司	641	41
三六零数字安全科技集团有限公司	396	396
上海交大	299	299
远江盛邦（北京）网络安全科技股份有限公司	139	139
南京众智维信息科技有限公司	90	2
北京升鑫网络科技有限公司（青藤云）	67	67
北京启明星辰信息安全技术有限公司	67	0
北京知道创宇信息技术有限公司	57	0
中国电信集团系统集成有限责任公司	17	0
快页信息技术有限公	16	16

司		
恒安嘉新（北京）科技股份公司	14	0
杭州迪普科技股份有限公司	10	0
杭州美创科技股份有限公司	8	8
华为技术有限公司	5	5
阿里云计算有限公司	4	4
北京长亭科技有限公司	4	2
北京智游网安科技有限公司	3	3
北京安信天行科技有限公司	1	1
成都卫士通信息安全技术有限公司	37	37
河南东方云盾信息技术有限公司	30	30
中孚安全技术有限公司	27	27
北京翰慧投资咨询有限公司	21	21
苏州棱镜七彩信息科技有限公司	15	15
淮安易云科技有限公司	14	14
贵州多彩网安科技有限公司	13	13
联通数字科技有限公司	12	12
北京纽盾网安信息技术有限公司	12	12
北京山石网科信息技术有限公司	10	10

江苏云天网络安全技术有限公司	9	9
江苏保旺达软件技术有限公司	8	8
上海维信荟智金融科技有限公司	5	5
成都安美勤信息技术股份有限公司	3	3
北京安帝科技有限公司	3	3
平安银河实验室	2	2
信息产业信息安全测评中心	2	2
中资网络信息安全科技有限公司	2	2
深圳昂楷科技有限公司	2	2
北京时代新威信息技术有限公司	2	2
北京君云天下科技有限公司	1	1
江苏金盾检测技术股份有限公司	1	1
中国工商银行	1	1
上海亿保健康科技集团有限公司	1	1
中国银行	1	1
江苏耘和计算机系统工程有限公司	1	1
超聚变数字技术有限公司	1	1
陕西青山四纪信息技术有限公司	1	1
江苏正信信息安全测试有限公司	1	1

上海吨吨信息技术有限公司	1	1
国网江西省电力有限公司电力科学研究院	1	1
武汉绿色网络股份有限责任公司	1	1
国家计算机病毒应急处理中心	1	1
CNCERT 贵州分中心	3	3
CNCERT 内蒙古分中心	2	2
CNCERT 湖南分中心	1	1
个人	831	831
报送总计	9330	3972

本周漏洞按类型和厂商统计

本周，CNVD 收录了 445 个漏洞。WEB 应用 199 个，操作系统 78 个，网络设备（交换机、路由器等网络端设备）74 个，应用程序 68 个，智能设备（物联网终端设备）22 个，安全产品 3 个，数据库 1 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	199
操作系统	78
网络设备（交换机、路由器等网络端设备）	74
应用程序	68
智能设备（物联网终端设备）	22
安全产品	3
数据库	1

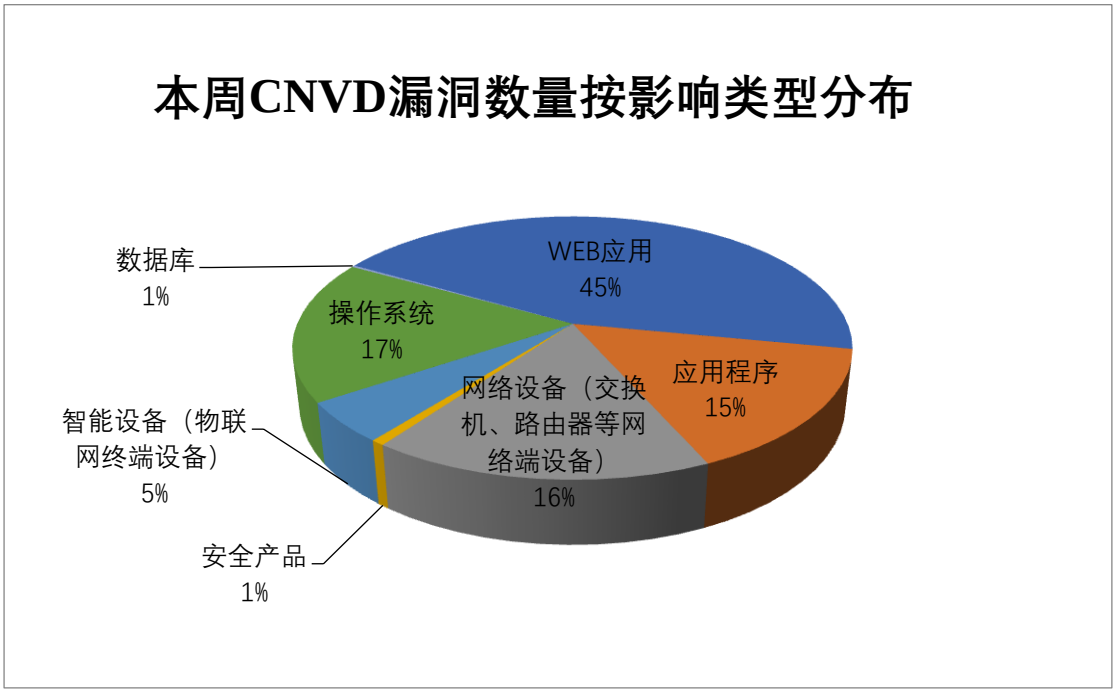

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、IrfanView、Google 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	65	15%
2	IrfanView	20	4%
3	Google	14	3%
4	畅捷通信息技术股份有限公司	12	3%
5	Siemens	10	2%
6	DELL	9	2%
7	北京金和网络股份有限公司	9	2%
8	Mozilla	8	2%
9	用友网络科技股份有限公司	8	2%
10	其他	290	65%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，3 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“mySCADA myPRO Manager 操作系统命令注入漏洞、Siemens Tecnomatix Plant Simulation 内存错误引用漏洞”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/

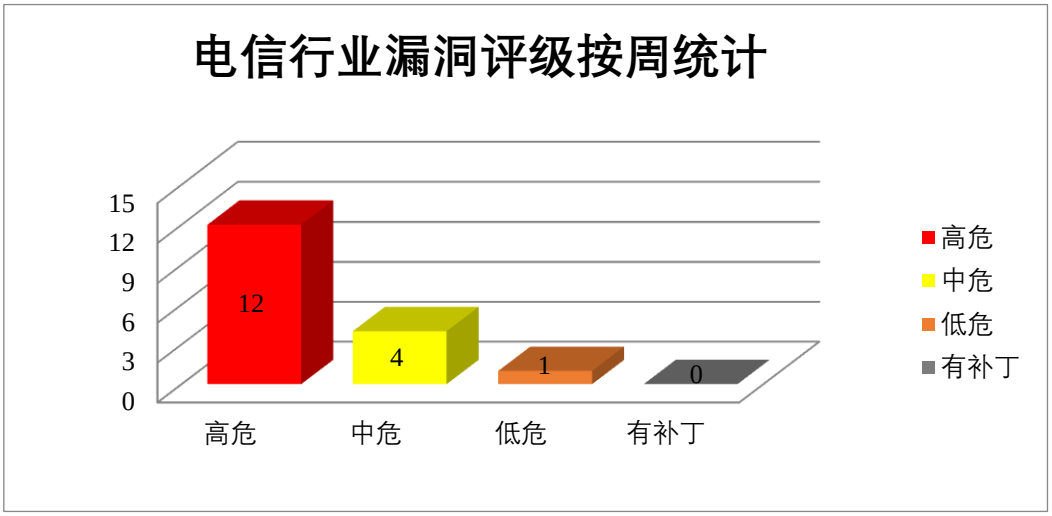

图 3 电信行业漏洞统计

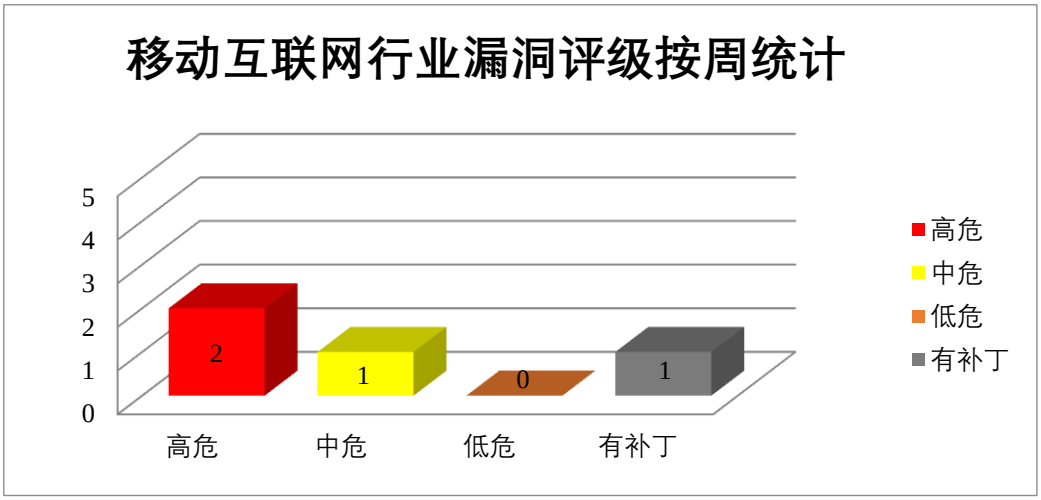

图 4 移动互联网行业漏洞统计

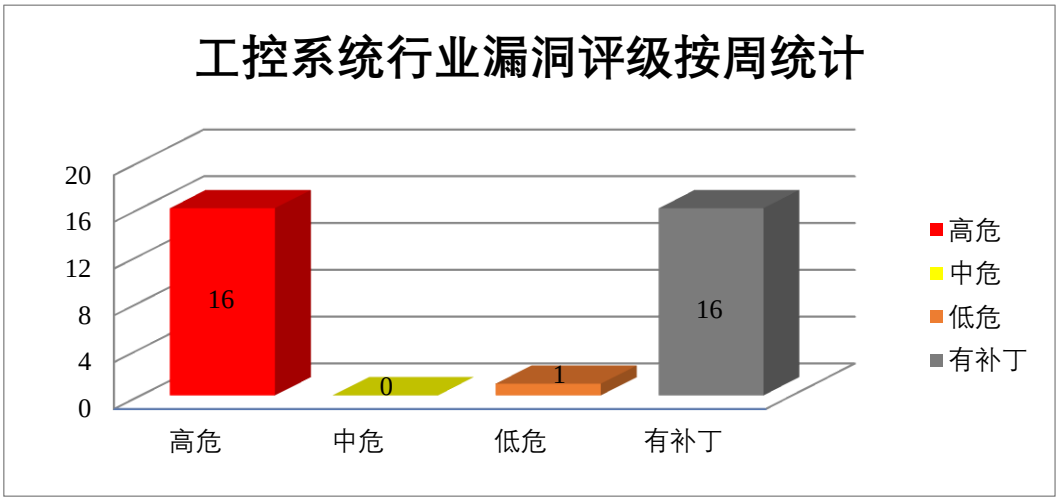

图 5 工控系统行业漏洞统计

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、 Mozilla 产品安全漏洞

Mozilla Firefox 等都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取基于 cookie 的身份验证凭据，在易受攻击的系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Mozilla Thunderbird 越界读取漏洞、Mozilla Firefox 和 Mozilla Thunderbird 跨站脚本漏洞、Mozilla Firefox 和 Mozilla Thunderbird 释放后重用漏洞、Mozilla 多款产品类型混淆漏洞、Mozilla 多款产品释放后重用漏洞（CNVD-2024-45879、CNVD-2024-45877）、Mozilla 多款产品访问控制错误漏洞、Mozilla Firefox 和 Mozilla Thunderbird 缓冲区溢出漏洞。其中，除“Mozilla Firefox 和 Mozilla Thunderbird 跨站脚本漏洞”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-2024-45875
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45874
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45873
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45880
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45879
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45878
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45877
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45876

2、 DELL 产品安全漏洞

Dell Enterprise SONiC OS 是美国戴尔（Dell）公司的一个开源网络操作系统。Dell ThinOS 是一个客户端操作系统。SmartFabric OS10 是一款专为现代数据中心织网络设计的先进操作系统，旨在简化管理、增强安全性和提升性能，为云计算和边缘计算环境提供强大而灵活的基础。Dell Data Lakehouse 是一个完全集成的数据平台。Dell BIOS 是一个计算机主板上小型内存芯片上的嵌入式软件。Dell Unity 是一种功能强大的存储解决方案，适用于中型企业和分支机构，提供高性能、可靠性和易用性，以满足企业对数据存储和管理的需求。Dell PowerProtect Data Domain（Dell PowerProtect DD）是一套用于数据保护、备份、存储和重复数据消除的硬件设备。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保护机制绕过，获得升级的权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Dell Enterprise SONiC OS 操作系统命令注入漏洞、Dell ThinOS 命令注入漏洞、Dell SmartFabric OS10 命令注入漏洞、Dell Data Lakehouse 访问控制错误漏洞、Dell Enterprise SONiC OS 身份验证错误漏洞、Dell BIOS 输入验证错误漏洞（CNVD-2024-46270）、Dell Unity 跨站脚本漏洞（CNVD-2024-46269）、Dell PowerProtect Data Domain 路径遍历漏洞。其中，除“Dell Data Lakehouse 访问控制错误漏洞、Dell Unity 跨站脚本漏洞（CNVD-2024-46269）、Dell PowerProtect Data Domain 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-2024-46262
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46266
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46265
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46264
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46263
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46270
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46269
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46268

3、Siemens 产品安全漏洞

Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。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进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2024-45988、CNVD-2024-45990、CNVD-2024-45989、CNVD-2024-45992、CNVD-2024-45993、CNVD-2024-45995）、Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2024-45991、CNVD-2024-45994）。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-2024-45988
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45990
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45989
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45992
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45991
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45994
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45993

https://www.cnvd.org.cn/flaw/show/CNVD-2024-45995

4、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，攻击者可利用漏洞获取敏感信息并在系统上执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Linux kernel 越界读取漏洞（CNVD-2024-45872、CNVD-2024-45870、CNVD-2024-45903）、Linux kernel 空指针解引用漏洞（CNVD-2024-45902、CNVD-2024-45904、CNVD-2024-45906、CNVD-2024-45905、CNVD-2024-45908）。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-2024-45872
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45870
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45903
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45902
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45904
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45906
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45905
https://www.cnvd.org.cn/flaw/show/CNVD-2024-45908

5、Apache Zeppelin 跨站请求伪造漏洞

Apache Zeppelin 是美国阿帕奇（Apache）基金会的一款基于 Web 的开源笔记本应用程序。该程序支持交互式数据分析和协作文档。本周，Apache Zeppelin 被披露存在跨站请求伪造漏洞。攻击者可以利用该漏洞造成跨站请求伪造。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-2024-46277

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-2024-45888	Google Pixel syscall.c 文件缓冲区溢出漏洞	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/pixel/2024-10-01
CNVD-2024-45987	Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞（CNVD-2024-45987）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-824503.html

CNVD-2024-46250	Palo Alto Networks PAN-OS 操作系统命令注入漏洞（CNVD-2024-46250）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.paloaltonetworks.com/CVE-2024-9474
CNVD-2024-46271	Apache OFBiz 代码问题漏洞（CNVD-2024-46271）	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/022r19skfofhv3lzql33vowlrvqndh11
CNVD-2024-46272	Apache Traffic Server 输入验证错误漏洞（CNVD-2024-46272）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://lists.apache.org/thread/y15fh6c7kyqvzm0f9odw7c5jh4r4np0y
CNVD-2024-46372	IrfanView 越界读取漏洞（CNVD-2024-46372）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.irfanview.com/
CNVD-2024-46380	IrfanView 越界写入漏洞（CNVD-2024-46380）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.irfanview.com/
CNVD-2024-46401	IBM Flexible Service Processor 信任管理问题漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.ibm.com/support/pages/node/7174183
CNVD-2024-46405	mySCADA myPRO Manager 目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.myscada.org/resources/
CNVD-2024-46433	TRCore DVC 文件上传漏洞（CNVD-2024-46433）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.trcore.com.tw/en

小结：本周，Mozilla 产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取基于 cookie 的身份验证凭据，在易受攻击的系统上执行任意代码或导致拒绝服务等。此外，DELL、Siemens、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致保护机制绕过，获取敏感信息并在系统上执行任意代码，导致拒绝服务等。另外，Apache Zeppelin 被披露存在跨站请求伪造漏洞。攻击者可以利用该漏洞造成跨站请求伪造。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、TP-LINK TL-WDR7660 缓冲区溢出漏洞

验证描述

TP-LINK TL-WDR7660 是中国普联（TP-LINK）公司的一款千兆路由器。

TP-LINK TL-WDR7660 1.0 版本存在缓冲区溢出漏洞，该漏洞源于 guestRuleJsonTobin 函数在处理参数字符串名称时未进行检查，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。

验证信息

POC 链接：https://github.com/sezangel/IOT-vul/tree/main/TPlink/TL-WDR7660/2

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-46444

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. Zabbix 发现 SQL 注入漏洞(CVE-2024-42327)，影响全球用户

Zabbix 是一款广泛使用的开源 IT 基础设施监控工具，近日发现其存在一个 SQL 注入漏洞(CVE-2024-42327)。

参考链接：https://starmap.dbappsecurity.com.cn/info/8981

2. Advantech 工业 WiFi 接入点被曝存在 20 多个漏洞

Advantech 工业级无线接入点设备被曝光存在近二十个安全漏洞，部分漏洞可被恶意利用以绕过身份验证并执行高权限代码。

参考链接：https://www.freebuf.com/news/416495.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