国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 08 月 12 日-2024 年 08 月 18 日 **2024 年第 33 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 246 个，其中高危漏洞 130 个、中危漏洞 107 个、低危漏洞 9 个。漏洞平均分值为 6.90。本周收录的漏洞中，涉及 0day 漏洞 144 个（占 59%），其中互联网上出现“Bike Delivery System SQL 注入漏洞、Record Management System sort 参数跨站脚本漏洞”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 27939 个，与上周（26411 个）环比减少 6%。

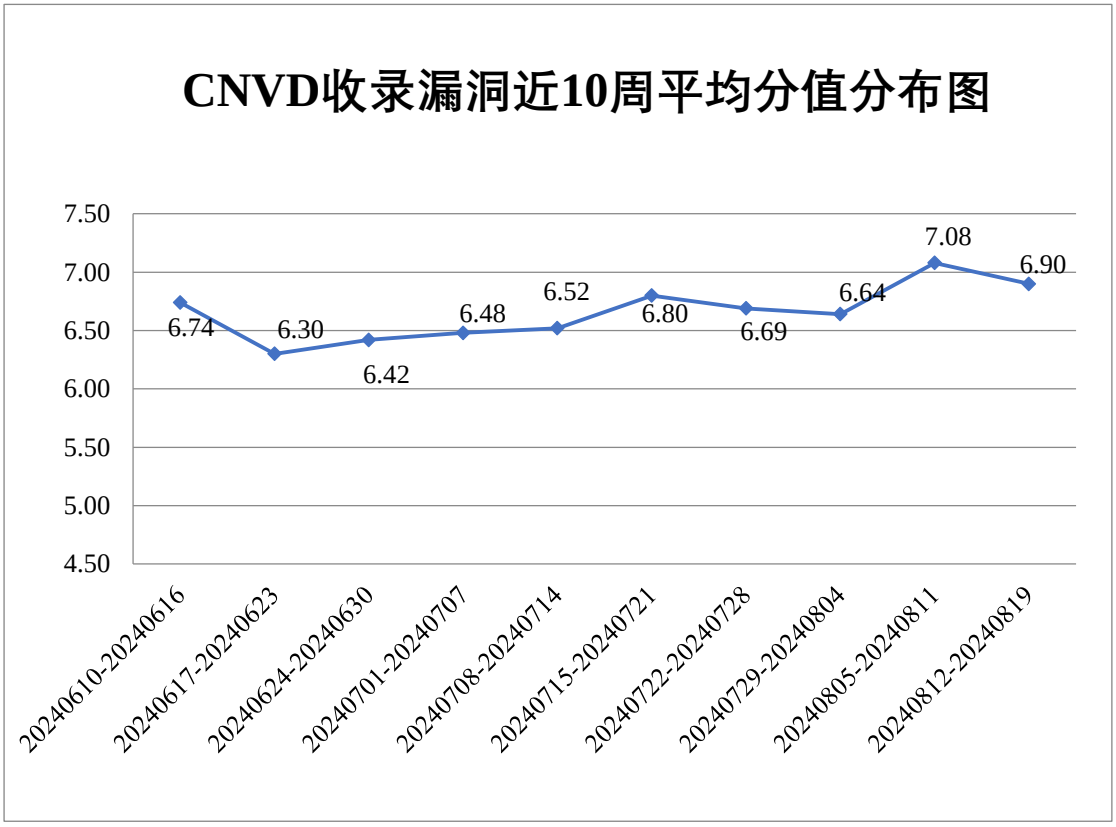

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向基础电信企业通报漏洞事件 1 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 679 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 48 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 10 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：

紫光股份有限公司、重庆米未科技有限公司、浙江宇视科技有限公司、浙江和达科技股份有限公司、昱能科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、译筑信息科技（上海）有限公司、烟台开发区德联软件有限责任公司、熊猫智慧水务有限公司、新天科技股份有限公司、微软（中国）有限公司、苏州科达科技股份有限公司、搜狗公司、深圳拓安信物联股份有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳达实物联网技术有限公司、上海真兰仪表科技股份有限公司、上海易路软件有限公司、上海三高计算机中心股份有限公司、上海脉感科技有限公司、上海肯特仪表股份有限公司、上海汉得信息技术股份有限公司、上海海鼎信息工程股份有限公司、上海泛微网络科技股份有限公司、青岛三利集团有限公司、南京帆软软件有限公司、酷溜网（北京）科技有限公司、京瓷办公信息系统（中国）有限公司、江苏鑫亿软件股份有限公司、佳能（中国）有限公司、湖南众合百易信息技术有限公司、杭州雄伟科技开发股份有限公司、海南汇成百年教育科技有限公司、广联达科技股份有限公司、福建科立讯通信有限公司、东方网力科技股份有限公司、成都天问互联科技有限公司、畅捷通信息技术股份有限公司、博锐尚格科技股份有限公司、北京用友政务软件股份有限公司、北京星网锐捷网络技术有限公司、北京鑫锐诚毅数字科技有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京美特软件技术有限公司、北京金万维科技有限公司、北京金和网络股份有限公司、北京华科仪科技股份有限公司、北京百卓网络技术有限公司、安元科技股份有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽科迅教育装备集团有限公司、安歌科技（集团）股份有限公司、爱普生（中国）有限公司、SEACMS 和 NETGEAR。

本周，CNVD 发布了《Microsoft 发布 2024 年 8 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/10316

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、新华三技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。河南东方云盾信息技术有限公司、马鞍山书拓安全科技有限公司、江苏金盾检测技术股份有限公司、快页信息技术有限公司、北京翰慧投资咨询有限公司、重庆都会信息科技、江苏晟晖信息科技有限公司、星云博创科技有限公司、江苏锋刃信息科技有限公司、杭州海康威视数字技术股份有限公司、江苏极元信息技术有限公司、甘肃赛飞安全科技有限公司、中国科学院计算机网络信息中心及其他个人白帽子向 CNVD 提交了 27939 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）、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 27353 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）	16182	16182
奇安信网神（补天平台）	10404	10404
北京天融信网络安全技术有限公司	1574	7
北京神州绿盟科技有限公司	1206	0
北京启明星辰信息安全技术有限公司	1121	0
三六零数字安全科技集团有限公司	601	601
新华三技术有限公司	543	0
深信服科技股份有限公司	305	0
安天科技集团股份有限公司	217	0
上海交大	166	166
京东科技信息技术有限公司	139	0
阿里云计算有限公司	132	2
杭州安恒信息技术股份有限公司	109	87
恒安嘉新（北京）科	56	0

技股份公司		
杭州迪普科技股份有限公司	32	2
南京众智维信息科技有限公司	26	26
北京知道创宇信息技术有限公司	21	0
北京安信天行科技有限公司	13	13
远江盛邦（北京）网络安全科技股份有限公司	13	13
中国电信集团系统集成有限责任公司	7	7
河南东方云盾信息技术有限公司	27	27
马鞍山书拓安全科技有限公司	25	25
江苏金盾检测技术股份有限公司	23	23
西门子（中国）有限公司	22	0
快页信息技术有限公司	10	10
F5	9	0
北京翰慧投资咨询有限公司	7	7
重庆都会信息科技	3	3
江苏晟晖信息科技有限公司	3	3
星云博创科技有限公司	2	2
江苏锋刃信息科技有限公司	1	1
杭州海康威视数字技	1	1

术股份有限公司		
江苏极元信息技术有限公司	1	1
甘肃赛飞安全科技有限公司	1	1
中国科学院计算机网络信息中心	1	1
CNCERT 福建分中心	3	3
CNCERT 贵州分中心	1	1
个人	320	320
报送总计	33327	27939

本周漏洞按类型和厂商统计

本周，CNVD 收录了 246 个漏洞。WEB 应用 130 个，应用程序 55 个，网络设备（交换机、路由器等网络端设备）45 个，智能设备（物联网终端设备）10 个，操作系统 4 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	130
应用程序	55
网络设备（交换机、路由器等网络端设备）	45
智能设备（物联网终端设备）	10
操作系统	4
数据库	2

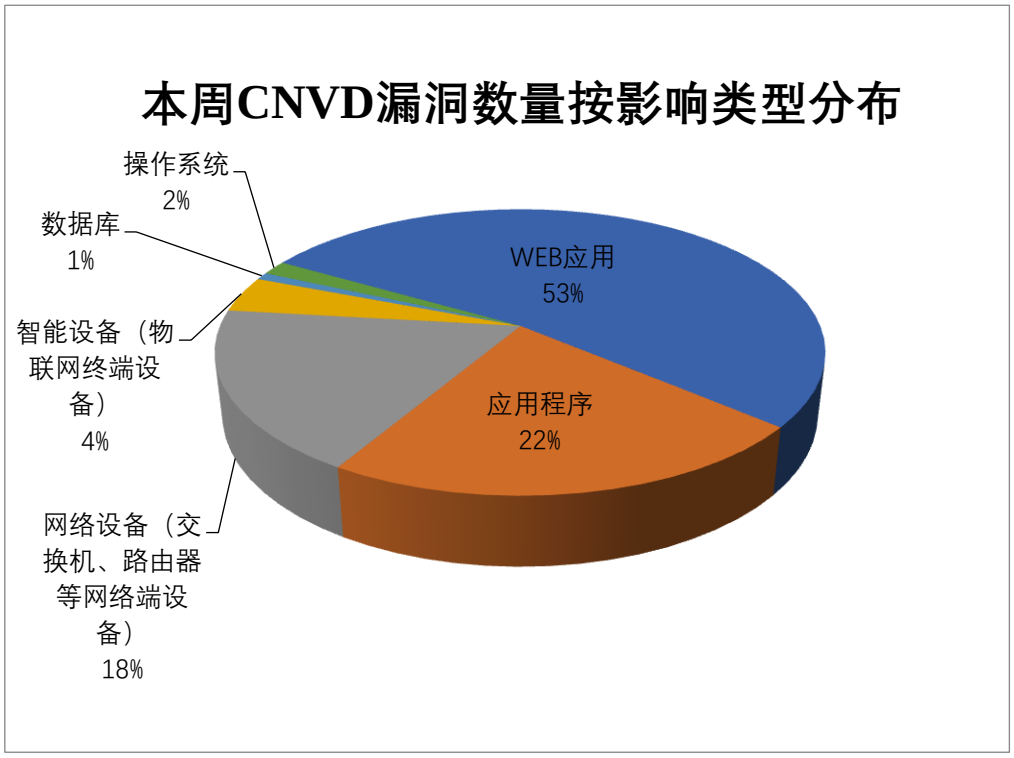

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Google、IBM 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	Siemens	23	9%
2	Google	15	6%
3	IBM	15	6%
4	Apache	9	4%
5	TOTOLINK	9	4%
6	DerbyNet	8	3%
7	Adobe	8	3%
8	北京神州视翰科技有限公司	7	3%
9	深圳市蓝凌软件股份有限公司	5	2%
10	其他	147	60%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，1 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“NETGEAR RAX30 命令注入漏洞（CNVD-2024-351

78）、Siemens SCALANCE M-800 系列输入验证错误漏洞”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/

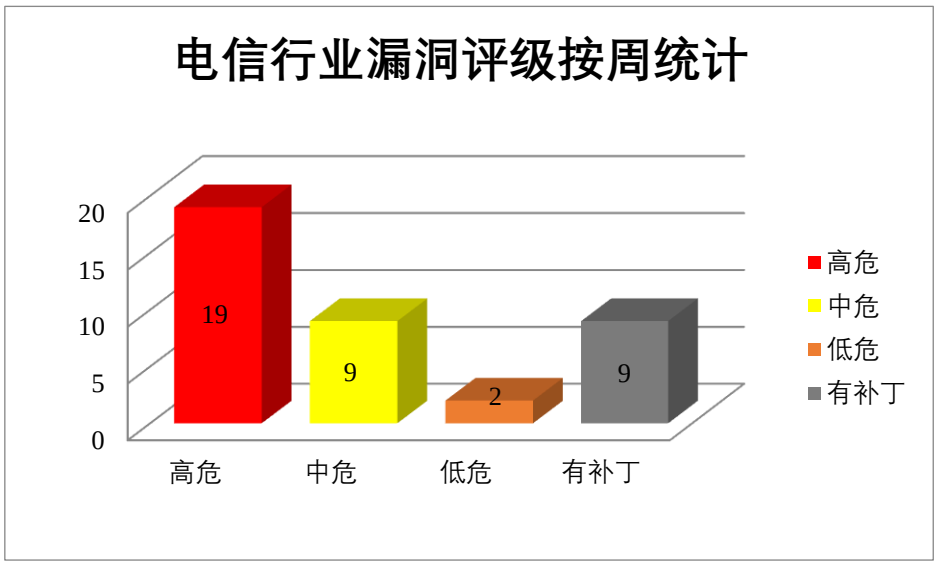

图 3 电信行业漏洞统计

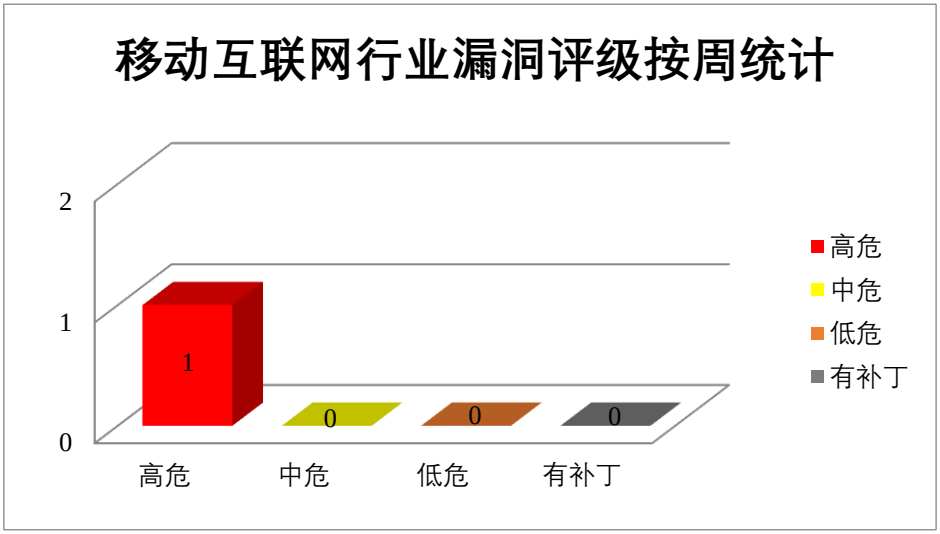

图 4 移动互联网行业漏洞统计

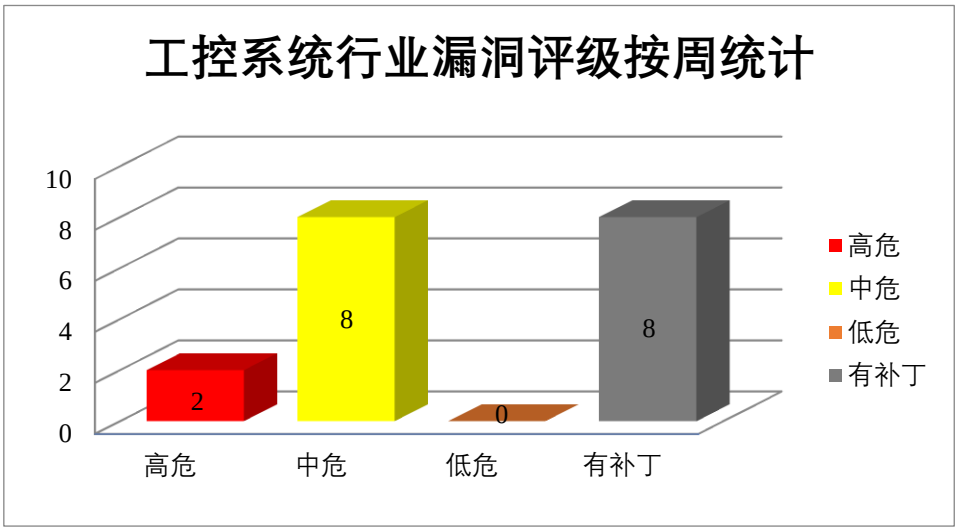

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Planning Analytics Local 是美国国际商业机器（IBM）公司的一个基于网络的本地架构。IBM Engineering Requirements Management DOORS Web Access 是美国国际商业机器（IBM）公司的一个工程需求管理软件。IBM System Management for i 是美国国际商业机器（IBM）公司的一个管理系统。IBM FlashSystem 5300 是美国国际商业机器（IBM）公司的一个将数据存储在闪存上的 IBM 存储企业系统。IBM Cloud Pak for Business Automation 是美国国际商业机器（IBM）公司的一组模块化的集成软件组件，专为任何混合云而构建，旨在实现工作自动化和加速业务增长。IBM Aspera Orchestrator 是美国国际商业机器（IBM）公司的一个基于 Web 的应用程序。可为数据驱动型企业提供高效的文件处理管道。IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。IBM Security Verify Directory 和 IBM Security Directory Integrator 都是美国国际商业机器（IBM）公司的产品。IBM Security Verify Directory 是一款身份验证和访问管理解决方案的一部分。IBM Security Directory Integrator 是一个集成开发环境和运行时服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权访问数据库，导致用户控制的代码以管理员权限运行，执行恶意和未经授权的操作等。

CNVD 收录的相关漏洞包括：IBM Planning Analytics Local 身份认证错误漏洞、IBM Engineering Requirements Management DOORS Web Access XML 外部实体注入漏洞、IBM System Management for i 代码问题漏洞、IBM FlashSystem 5300 身份验证错误漏洞、IBM Cloud Pak for Business Automation 服务器端请求伪造漏洞、IBM As

pera Orchestrator 跨站请求伪造漏洞、IBM InfoSphere Information Server SQL 注入漏洞（CNVD-2024-35171）、IBM Security Verify Directory/Directory Integrator 访问控制错误漏洞。其中，“IBM Engineering Requirements Management DOORS Web Access XML 外部实体注入漏洞、IBM System Management for i 代码问题漏洞、IBM Aspera Orchestrator 跨站请求伪造漏洞、IBM InfoSphere Information Server SQL 注入漏洞（CNVD-2024-35171）”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-2024-35112
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35114
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35119
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35118
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35117
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35167
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35171
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35174

2、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。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，使溢出缓冲区，在系统上执行任意代码或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2024-35258、CNVD-2024-35260）、Google Chrome 安全绕过漏洞（CNVD-2024-35259）、Google Chrome 缓冲区溢出漏洞（CNVD-2024-35261）、Google Chrome 内存错误引用漏洞（CNVD-2024-35262、CNVD-2024-35263、CNVD-2024-35264、CNVD-2024-35265）。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-2024-35258
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35259
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35260
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35261
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35262
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35263
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35264
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35265

3、 Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构

建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML 等。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-35195、CNVD-2024-35194、CNVD-2024-35198、CNVD-2024-35197、CNVD-2024-35196、CNVD-2024-35201、CNVD-2024-35200、CNVD-2024-35199）。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-2024-35195
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35194
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35198
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35197
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35196
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35201
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35200
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35199

4、Siemens 产品安全漏洞

Omnivise T3000 是一种分布式控制系统，主要用于化石燃料和大型可再生能源发电厂。SINEC NMS 是面向数字化企业的新一代网络管理系统。SINEC Traffic Analyzer 是一个内部部署的应用程序，监控控制器和 IO 设备之间的 PNIO (PROFINET IO)通信。SCALANCE M-800，MUM-800，S615，RUGGEDCOM RM1224 都是是工业路由器。NX 是一个集成的工具集，通过支持产品开发的各个方面，使设计师能够优化形状以实现多学科设计，帮助开发设计，仿真和制造解决方案。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或消耗内存资源，对易受攻击的系统进行各种攻击，包括跨站点脚本、缓存中毒或会话劫持，绕过检查并提升在应用程序上的权限等。

CNVD 收录的相关漏洞包括：Siemens Omnivise T3000 Application Server 路径遍历漏洞、Siemens Omnivise T3000 Application Server 输入验证不当漏洞、Siemens SINEC NMS 授权错误漏洞、Siemens SINEC NMS 输入验证错误漏洞、Siemens SINEC Traffic Analyzer 权限管理错误漏洞、Siemens SINEC Traffic Analyzer 逻辑缺陷漏洞（CNVD-2024-35433）、Siemens SCALANCE M-800 系列配置错误漏洞、Siemens NX 越界读取漏洞。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-2024-35108
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35109
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35424

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35423

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35434

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35433

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35437

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35435

5、TOTOLINK A3002R 缓冲区溢出漏洞（CNVD-2024-35649）

TOTOLINK A3002R 是中国吉翁电子（TOTOLINK）公司的一款无线双频千兆路由器。本周，TOTOLINK A3002R 被披露存在缓冲区溢出漏洞。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。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-2024-35649

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-2024-35105	Apache OFBiz 授权错误漏洞	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/olxxjk6b13sl3wh9cmp0k2dscvp24l7w
CNVD-2024-35164	SiberianCMS SQL 注入漏洞（CNVD-2024-35164）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Xtraball/SiberianCMS
CNVD-2024-35168	ChurchCRM SQL 注入漏洞（CNVD-2024-35168）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ChurchCRM/CRM/security/advisories/GHSA-2rh6-gr3h-83j9
CNVD-2024-35170	Apache Traffic Server 输入验证错误漏洞（CNVD-2024-35170）	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/c4mcmpblgl8kkmyt56t23543gp8v56m0
CNVD-2024-35169	Apache Traffic Server 输入验证错误漏洞（CNVD-2024-35169）	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/c4mcmpblgl8kkmyt56t23543gp8v56m0
CNVD-2024-35177	Apache StreamPark 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/n6dhnl

			68knpxy80t35qxkkw2691l8sfn
CNVD-2024-35182	ThinkSAAS SQL 注入漏洞（CNVD-2024-35182）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.thinksaas.cn/
CNVD-2024-35256	Google Chrome Sharing 模块内存错误引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html
CNVD-2024-35558	Calibre 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://github.com/kovidgoyal/calibre/releases/tag/v7.16.0
CNVD-2024-35561	Mozilla Firefox 内存错误引用漏洞（CNVD-2024-35561）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2024-33/

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞未经授权访问数据库，导致用户控制的代码以管理员权限运行，执行恶意和未经授权的操作等。此外，Google、Adobe、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞注入精心设计的有效载荷执行任意 Web 脚本或 HTML，绕过安全限制，使溢出缓冲区，在系统上执行任意代码或导致应用程序崩溃等。另外，TOTOLINK A3002R 被披露存在缓冲区溢出漏洞。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。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、 Bike Delivery System SQL 注入漏洞

验证描述

Bike Delivery System 是一个自行车配送系统。

Bike Delivery System 1.0 版本存在 SQL 注入漏洞，该漏洞源于参数 name 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/CveSecLook/cve/issues/56

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-35156

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. 巴黎奥运会期间共发生超 140 起网络攻击事件

法国当局周二表示，在巴黎奥运会期间，共报告了超过 140 起网络攻击，但均未对比赛造成干扰。在奥运会筹备期间和整个比赛期间，法国的网络安全机构一直保持高度警戒，防范可能破坏组委会、票务或交通的攻击。

参考链接：https://www.secrss.com/articles/69185

2. Microsoft 禁用 BitLocker 安全修复，建议手动缓解

Microsoft 已禁用对 BitLocker 安全功能绕过漏洞的修复，这是由于固件不兼容问题导致修补的 Windows 设备进入 BitLocker 恢复模式。

参考链接：https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-bitlocker-security-fix-advises-manual-mitigation/

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