国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 05 月 20 日-2024 年 05 月 26 日 **2024 年第 21 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 583 个，其中高危漏洞 361 个、中危漏洞 207 个、低危漏洞 15 个。漏洞平均分值为 7.01。本周收录的漏洞中，涉及 0day 漏洞 492 个（占 84%），其中互联网上出现“Online Chatting System SQL 注入漏洞（CNVD-2024-23320）、Inventory Management System SQL 注入漏洞（CNVD-2024-23321）”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 7148 个，与上周（8468 个）环比减少 16%。

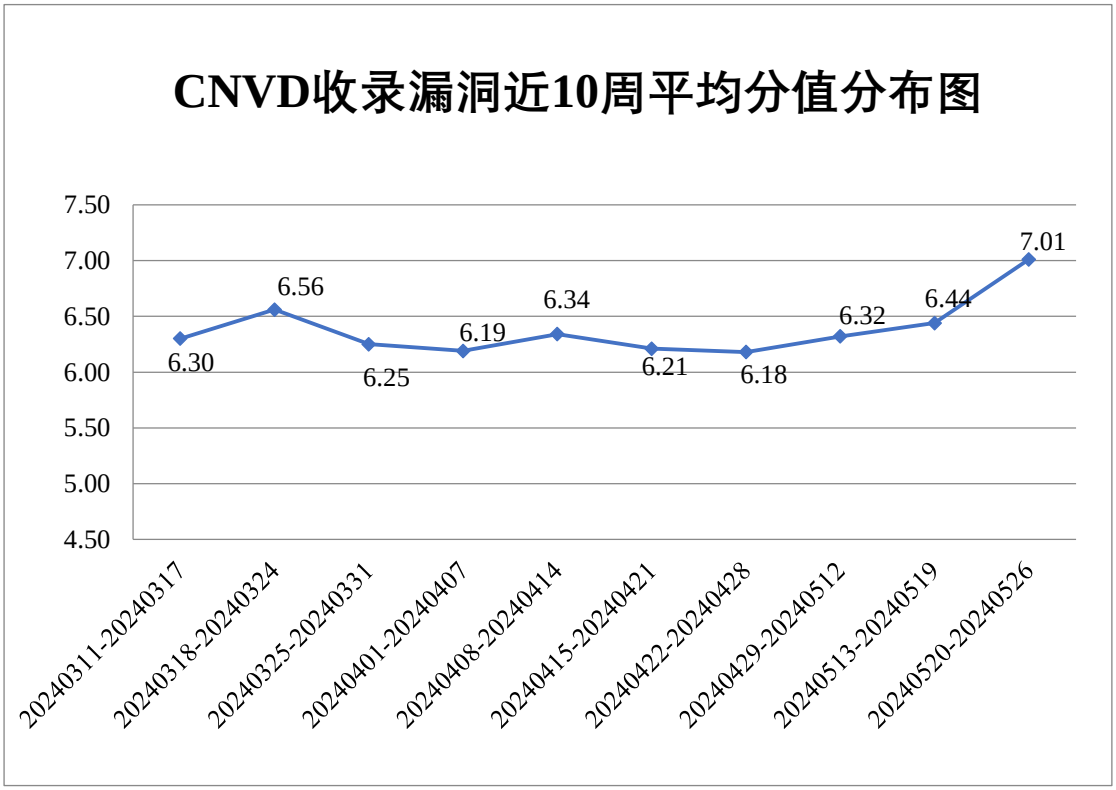

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 458 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 41 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 19 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：

紫光云技术有限公司、中国计算机学会、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、兄弟（中国）商业有限公司、行信通科技（内蒙古）有限责任公司、新中新集团、夏普科技（上海）有限公司、西安瑞友信息技术资讯有限公司、武汉城投停车场投资建设管理有限公司、无锡信捷电气股份有限公司、微软（中国）有限公司、统信软件技术有限公司、索尼（中国）有限公司、四川掌上时代科技有限公司、斯大精密（大连）有限公司、深圳市思迅软件股份有限公司、深圳市赛格导航科技股份有限公司、深圳市明源云科技有限公司、深圳市美科星通信技术有限公司、深圳市力必拓科技有限公司、深圳市吉祥腾达科技有限公司、深圳市河辰通讯技术有限公司、深圳市鼎游信息技术有限公司、深圳市必联电子有限公司、深圳前海华夏智信数据科技有限公司、上汽通用五菱汽车股份有限公司、上海卓卓网络科技有限公司、上海普华科技发展股份有限公司、上海华测导航技术股份有限公司、商派软件有限公司、厦门印天电子科技有限公司、厦门四信通信科技有限公司、厦门快普信息技术有限公司、厦门科拓通讯技术股份有限公司、青岛中瑞云数科技有限公司、青岛和正信息技术有限公司、麒麟软件有限公司、普元信息技术股份有限公司、平凯星辰（北京）科技有限公司、南宁迈世信息技术有限公司、南昌蓝智科技有限公司、南昌航天广信科技有限责任公司、隆昌三皮网络科技有限公司、联想（北京）有限公司、力合科技（湖南）股份有限公司、理光（中国）投资有限公司、昆明东讯科技有限公司、柯尼卡美能达集团、京源中科科技股份有限公司、京瓷办公信息系统（中国）有限公司、江西铭软科技有限公司、江苏赛达电子科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、怀化南山田舍科技有限公司、湖北点点点科技有限公司、恒亦明（重庆）科技有限公司、河北先河环保科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、杭州短趣网络传媒技术有限公司、汉王科技股份有限公司、哈尔滨新中新电子股份有限公司、广州市溢信科技股份有限公司、广州市飞帆计算机技术有限公司、广西众链网络科技有限公司、广联达科技股份有限公司、广东国星科技有限公司、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、福建亿同世纪软件科技股份有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、成都长益西联软件有限公司、成都惠生源软件有限公司、畅捷通信息技术股份有限公司、北京致远互联软件股份有限

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、北京小米科技有限责任公司、北京万户网络技术有限公司、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、北京玛格泰克科技发展有限公司、北京龙软科技股份有限公司、北京久其软件股份有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、百度安全应急响应中心、奥琦玮信息科技（北京）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、安徽中技国医医疗科技有限公司、安徽新中新华科电子有限公司、安徽共生物流科技有限公司、爱普生（中国）有限公司、seacms、pigcloud、Oki Electric Industry Co 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，新华三技术有限公司、北京启明星辰信息安全技术有限公司、北京天融信网络安全技术有限公司、北京数字观星科技有限公司、阿里云计算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、成都久信信息技术股份有限公司、北京神州泰岳软件股份有限公司、内蒙古中叶信息技术有限责任公司、快页信息技术有限公司、联想集团、北京中睿天下信息技术有限公司、北京天下信安技术有限公司、杭州海康威视数字技术股份有限公司、西藏闪锁网络科技有限公司、星云博创科技有限公司、中资网络信息安全科技有限公司、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、江苏极元信息技术有限公司、海南神州希望网络有限公司、湖南泛联新安信息科技有限公司、苏州棱镜七彩信息科技有限公司、江苏晟晖信息科技有限公司、河南天祺信息安全技术有限公司、北京天防安全科技有限公司、江苏金盾检测技术股份有限公司、广西网信信息技术有限公司、上海观安信息技术股份有限公司、北京星网锐捷网络技术有限公司、中国电信股份有限公司上海研究院、四川云盛安科技有限公司、厦门聚丁科技有限公司、中孚安全技术有限公司、贵州华黔信安信息技术有限公司、北银金融科技有限责任公司、国网山东省电力公司、上海直画科技有限公司、中电福富信息科技有限公司、联通数字科技有限公司、广电计量检测集团股份有限公司及其他个人白帽子向 CNVD 提交了 7148 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 5814 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）	3582	3582

奇安信网神（补天平台）	1726	1726
新华三技术有限公司	1462	0
北京启明星辰信息安全技术有限公司	520	2
北京天融信网络安全技术有限公司	252	25
上海交大	265	265
三六零数字安全科技集团有限公司	241	241
北京数字观星科技有限公司	223	0
阿里云计算有限公司	162	0
恒安嘉新（北京）科技股份公司	85	0
华为技术有限公司	84	0
北京知道创宇信息技术有限公司	60	0
杭州安恒信息技术股份有限公司	55	55
远江盛邦（北京）网络安全科技股份有限公司	46	46
北京长亭科技有限公司	16	1
北京安信天行科技有限公司	12	12
北京智游网安科技有限公司	6	6
西安四叶草信息技术有限公司	4	4
中国电信集团系统集成有限责任公司	2	2
中国电信股份有限公司网络安全产品运营	1	1

中心		
河南东方云盾信息技术有限公司	49	49
马鞍山书拓安全科技有限公司	29	29
成都久信信息技术股份有限公司	16	16
北京神州泰岳软件股份有限公司	14	14
内蒙古中叶信息技术有限责任公司	14	14
快页信息技术有限公司	13	13
联想集团	12	12
北京中睿天下信息技术有限公司	11	11
北京天下信安技术有限公司	9	9
杭州海康威视数字技术股份有限公司	7	7
西藏闪锁网络科技有限公司	6	6
星云博创科技有限公司	5	5
中资网络信息安全科技有限公司	4	4
北京山石网科信息技术有限公司	3	3
重庆都会信息科技有限公司	3	3
江苏极元信息技术有限公司	3	3
海南神州希望网络有限公司	3	3
湖南泛联新安信息科	2	2

技有限公司		
苏州棱镜七彩信息科技有限公司	2	2
江苏晟晖信息科技有限公司	2	2
河南天祺信息安全技术有限公司	2	2
北京天防安全科技有限公司	2	2
江苏金盾检测技术股份有限公司	2	2
广西网信信息技术有限公司	1	1
上海观安信息技术股份有限公司	1	1
北京星网锐捷网络技术有限公司	1	1
中国电信股份有限公司上海研究院	1	1
四川云盛安科技有限公司	1	1
厦门聚丁科技有限公司	1	1
中孚安全技术有限公司	1	1
贵州华黔信安信息技术有限公司	1	1
北银金融科技有限责任公司	1	1
国网山东省电力公司	1	1
上海直画科技有限公司	1	1
中电福富信息科技有限公司	1	1
联通数字科技有限公	1	1

司		
广电计量检测集团股份有限公司	1	1
CNCERT 宁夏分中心	12	12
CNCERT 河北分中心	5	5
个人	936	936
报送总计	9984	7148

本周漏洞按类型和厂商统计

本周，CNVD 收录了 583 个漏洞。WEB 应用 346 个，网络设备（交换机、路由器等网络端设备）110 个，应用程序 82 个，智能设备（物联网终端设备）32 个，操作系统 11 个，安全产品 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	346
网络设备（交换机、路由器等网络端设备）	110
应用程序	82
智能设备（物联网终端设备）	32
操作系统	11
安全产品	2

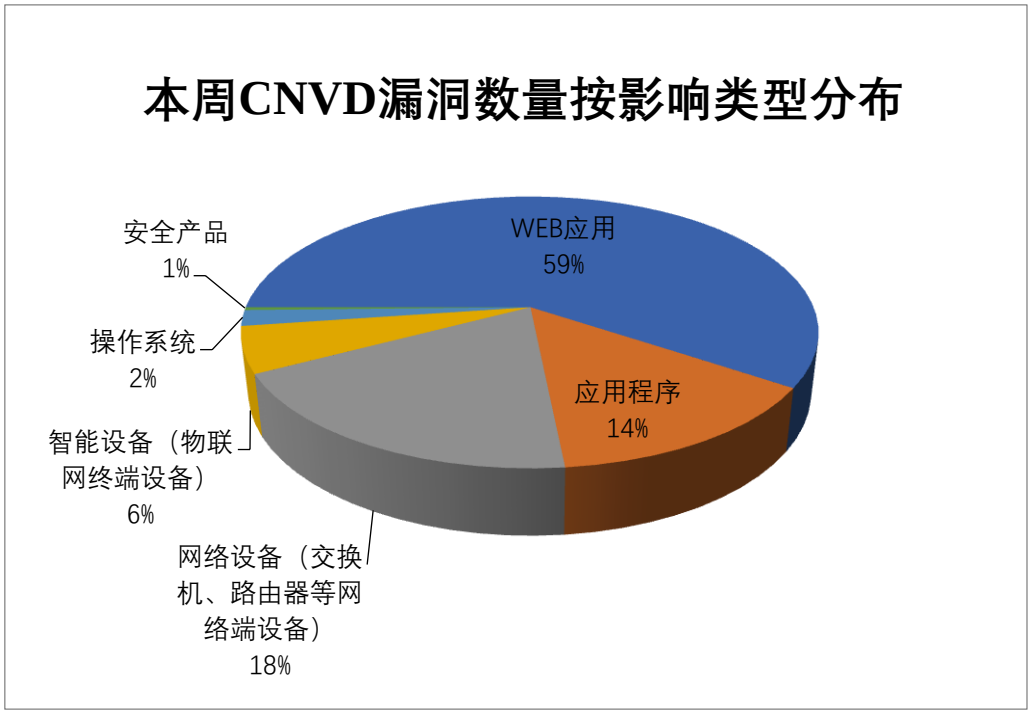

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用 Tenda、北京星网锐捷网络技术有限公司、Mozilla 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	Tenda	27	5%
2	北京星网锐捷网络技术有限公司	21	4%
3	Mozilla	16	2%
4	用友网络科技股份有限公司	14	2%
5	Siemens	13	2%
6	福建科立讯通信有限公司	13	2%
7	北京神州视翰科技有限公司	10	2%
8	SAP	10	2%
9	H3C	10	2%
10	其他	449	77%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，18 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，“Tenda TX9 Pro sub_42CB94 方法缓冲区溢出漏洞、Mozilla Firefox for Android 欺骗漏洞（CNVD-2024-23342）”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/

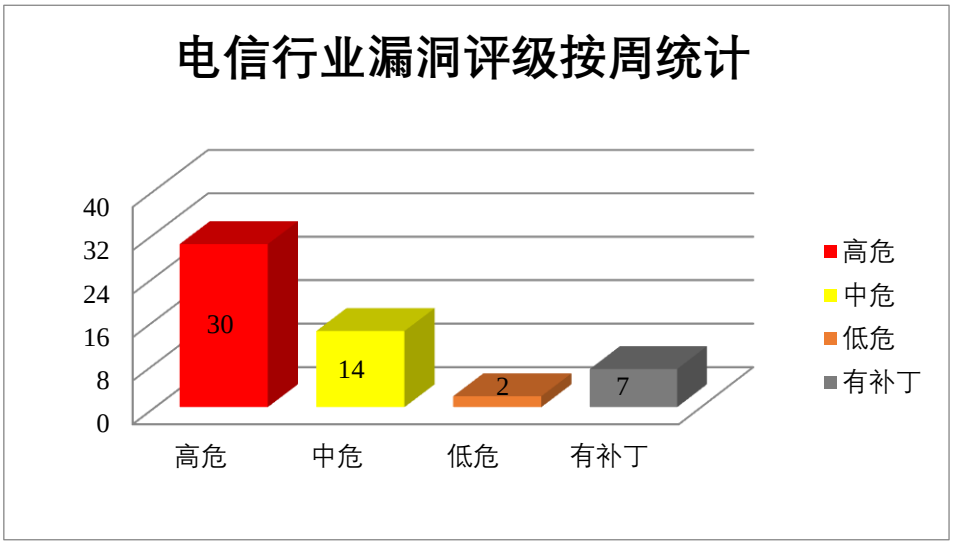

图 3 电信行业漏洞统计

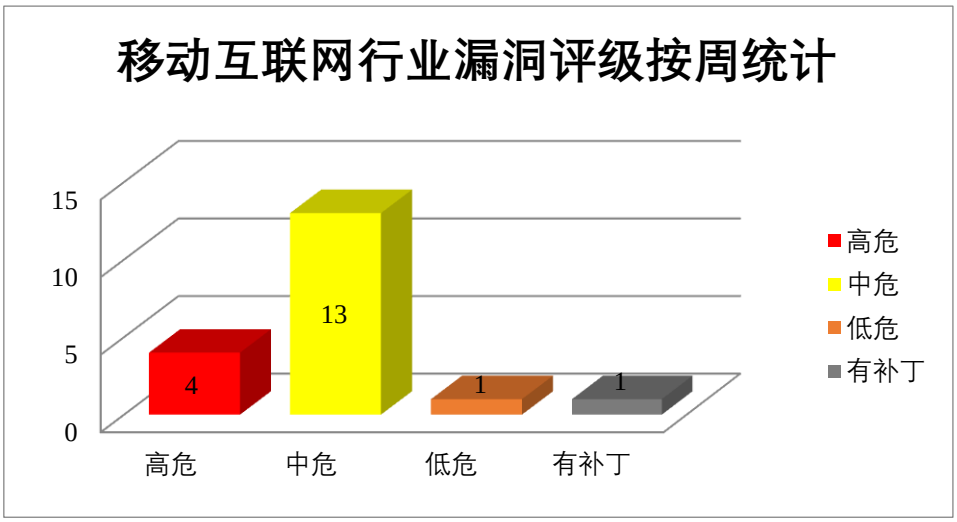

图 4 移动互联网行业漏洞统计

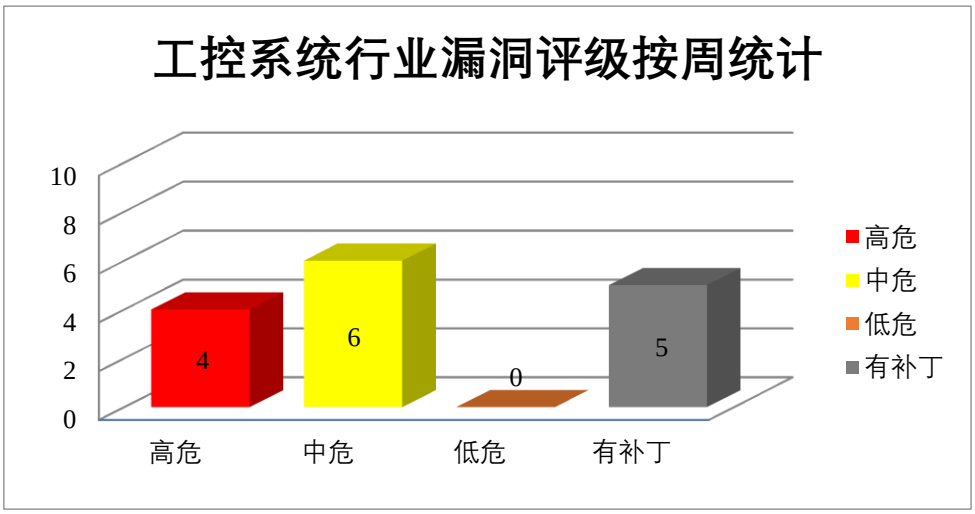

图 5 工控系统行业漏洞统计

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 是美国 Mozilla 基金会的一款开源 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，获取敏感信息，执行任意代码或导致拒绝服务。

CNVD 收录的相关漏洞包括：Mozilla Firefox 拒绝服务漏洞（CNVD-2024-23334、CNVD-2024-23335）、Mozilla Firefox 代码执行漏洞（CNVD-2024-23337、CNVD-2024-23341、CNVD-2024-23340、CNVD-2024-23339）、Mozilla Firefox 信息泄露漏洞（CNVD-2024-23336）、Mozilla Firefox 安全绕过漏洞（CNVD-2024-23344）。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-2024-23334

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23337

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23336

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23335

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23341

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23340

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23339

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23344

2、 Siemens 产品安全漏洞

Simcenter Nastran 是一款有限元法求解器。Siemens Solid Edge 是德国西门子（Siemens）公司的一款三维 CAD 软件。该软件可用于零件设计、装配设计、钣金设计、焊接设计等行业。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。Siemens JT2Go 是一款 JT 文件查看器。Siemens RUGGEDCOM CROSSBOW 是德国西门子（Siemens）公司的一个经过验证的安全访问管理解决方案。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数据库敏感信息，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 Simcenter Nastran 堆栈缓冲区溢出漏洞、Siemens Solid Edge 越界读取漏洞（CNVD-2024-23519、CNVD-2024-23520、CNVD-2024-23522）、Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2024-23521）、Siemens Teamcenter Visualization 和 JT2Go 堆栈缓冲区溢出漏洞（CNVD-2024-23523）、Siemens Teamcenter Visualization 和 JT2Go 越界写入漏洞（CNVD-2024-23524）、Siemens RUG

GEDCOM CROSSBOW SQL 注入漏洞。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-2024-23515
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23519
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23520
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23521
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23522
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23523
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23524
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23527

3、IBM 产品安全漏洞

IBM AIX 是美国国际商业机器（IBM）公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM Cognos Controller 是美国国际商业机器（IBM）公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。IBM Engineering Requirements Management DOORS 是一个需求管理工具。IBM FileNet Content Manager 是美国国际商业机器（IBM）公司的一套针对 FileNet P8 平台的内容管理解决方案。该方案将文档管理与即用型工作流程工具相结合，可管理图像、视频、Web 内容、合规性文档等。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，发送特制的 SQL 语句，从而查看、添加、修改或删除后端数据库中的信息，在 Web UI 中嵌入任意 JavaScript 代码等。

CNVD 收录的相关漏洞包括：IBM AIX 权限提升漏洞（CNVD-2024-23284）、IBM Cognos Controller 信息泄露漏洞（CNVD-2024-23286）、IBM Cognos Controller SQL 注入漏洞、IBM Engineering Requirements Management DOORS 跨站脚本漏洞、IBM Engineering Requirements Management DOORS 跨站请求伪造漏洞、IBM FileNet Content Manager 权限许可和访问控制问题漏洞、IBM Cognos Controller 用户枚举漏洞、IBM Security Guardium Key Lifecycle Manager 文件上传漏洞。其中，“IBM Cognos Controller SQL 注入漏洞、IBM Engineering Requirements Management DOORS 跨站请求伪造漏洞” 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-2024-23284
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23286
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23285
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23290
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23289

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23288

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23287

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23292

4、SAP 产品安全漏洞

SAP Master Data Governance 是德国思爱普（SAP）公司的一套用于维护、验证和分发主数据的数据管理工具。SAP PowerDesigner 是德国思爱普（SAP）公司的一款数据库设计软件。SAP macOS-enterprise-privileges 是德国思爱普（SAP）公司的一款应用软件，可以提供一种快速、简单的方法在需要时获取管理员权限。SAP Enable Now 是德国思爱普（SAP）公司的一套协作内容创作、管理和共享平台。该平台主要用于 SAP 和非 SAP 系统的在线学习和培训等。SAP Solution Manager 是德国思爱普(SAP)公司的一套系统监控，能方便对企业进行技术相关与应用相关功能的监控。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 Web Dispatcher 是德国思爱普（SAP）公司的 Load Balancing 的核心组件，支持负载均衡，提供反向代理的功能，使得外网用户可以访问到内部应用。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或劫持用户会话，执行任意代码，导致系统崩溃等。

CNVD 收录的相关漏洞包括：SAP Master Data Governance 授权问题漏洞、SAP PowerDesigner 代码注入漏洞（CNVD-2024-23328）、SAP macOS-enterprise-privileges 缓冲区溢出漏洞、SAP Enable Now 代码问题漏洞、SAP Solution Manager 跨站脚本漏洞（CNVD-2024-23331）、SAP NetWeaver AS 输入验证错误漏洞（CNVD-2024-23330）、SAP Web Dispatcher 缓冲区溢出漏洞、SAP Solution Manager 输入验证错误漏洞。其中，“SAP PowerDesigner 代码注入漏洞（CNVD-2024-23328）、SAP Web Dispatcher 缓冲区溢出漏洞”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-2024-23324

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23328

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23327

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23326

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23331

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23330

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23329

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23785

5、Cisco NX-OS Software 身份验证错误漏洞

Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。本周，Cisco NX-OS Software 被披露存在身份验证错误漏洞。攻击者可

利用该漏洞通过在登录提示符下输入特制的字符串来导致系统拒绝服务（DoS）。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-2024-23323

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-2024-23782	Tenda TX9 Pro sub_42C014 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4219.html
CNVD-2024-23289	IBM Engineering Requirements Management DOORS 跨站请求伪造漏洞	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/7124058
CNVD-2024-23308	FreeRDP NULL 指针解引用漏洞	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.freerdp.com/
CNVD-2024-23338	Mozilla Firefox 代码执行漏洞（CNVD-2024-23338）	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/mfsa2024-21/
CNVD-2024-23516	Siemens SIMATIC CN 4100 硬编码凭证漏洞	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://cert-portal.siemens.com/productcert/html/ssa-273900.html
CNVD-2024-23781	Tenda TX9 Pro sub_42BD7C 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4219.html
CNVD-2024-23285	IBM Cognos Controller 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.ibm.com/support/pages/node/7149876
CNVD-2024-23335	Mozilla Firefox 拒绝服务漏洞（CNVD-2024-23335）	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/mfsa2024-23/ https://www.mozilla.org/en-US/security/advisories/mfsa2024-22/

			https://www.mozilla.org/en-US/security/advisories/mfsa2024-21/
CNVD-2024-23517	Siemens SIMATIC CN 4100 硬编码密码漏洞	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://cert-portal.siemens.com/productcert/html/ssa-273900.html
CNVD-2024-23783	Tenda TX9 Pro sub_42CB94 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4219.html

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，获取敏感信息，执行任意代码或导致拒绝服务。此外，Siemens、IBM、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取数据库敏感信息，在当前进程的上下文中执行代码，导致系统崩溃等。另外，Cisco NX-OS Software 被披露存在身份验证错误漏洞。攻击者可利用该漏洞通过在登录提示符下输入特制的字符串来导致系统拒绝服务（DoS）。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、Online Chatting System SQL 注入漏洞（CNVD-2024-23320）

验证描述

Online Chatting System 是一个在线聊天系统。

Online Chatting System 1.0 版本存在 SQL 注入漏洞，该漏洞源于文件 admin/update_room.php 的参数 id 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/3

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-23320

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. GitLab 爆出安全漏洞，允许黑客接管账户

近日，GitLab 爆出一个安全漏洞（被追踪为 CVE-2024-4835），未经认证的威胁攻击者能够利用该漏洞在跨站脚本 (XSS) 攻击中，轻松接管受害者账户。

参考链接：https://www.freebuf.com/news/401772.html

2. 英特尔 AI 模型压缩器存在安全漏洞，可导致任意代码执行

据 Info risk today 消息，英特尔公司的人工智能模型压缩软件 Neural Compressor 中存在安全漏洞，该漏洞在 CVSS 的评分为 10 分，攻击者可以在运行受影响版本的系统上执行任意代码。

参考链接：https://www.freebuf.com/news/401448.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