国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 06 月 17 日-2024 年 06 月 23 日 **2024 年第 25 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 314 个，其中高危漏洞 129 个、中危漏洞 174 个、低危漏洞 11 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 62%），其中互联网上出现“J2EEFAST BpmTaskFromMapper.xml 文件 SQL 注入漏洞、Cesanta MJS 拒绝服务漏洞（CNVD-2024-27558）”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 14284 个，与上周（4795 个）环比增长 198%。

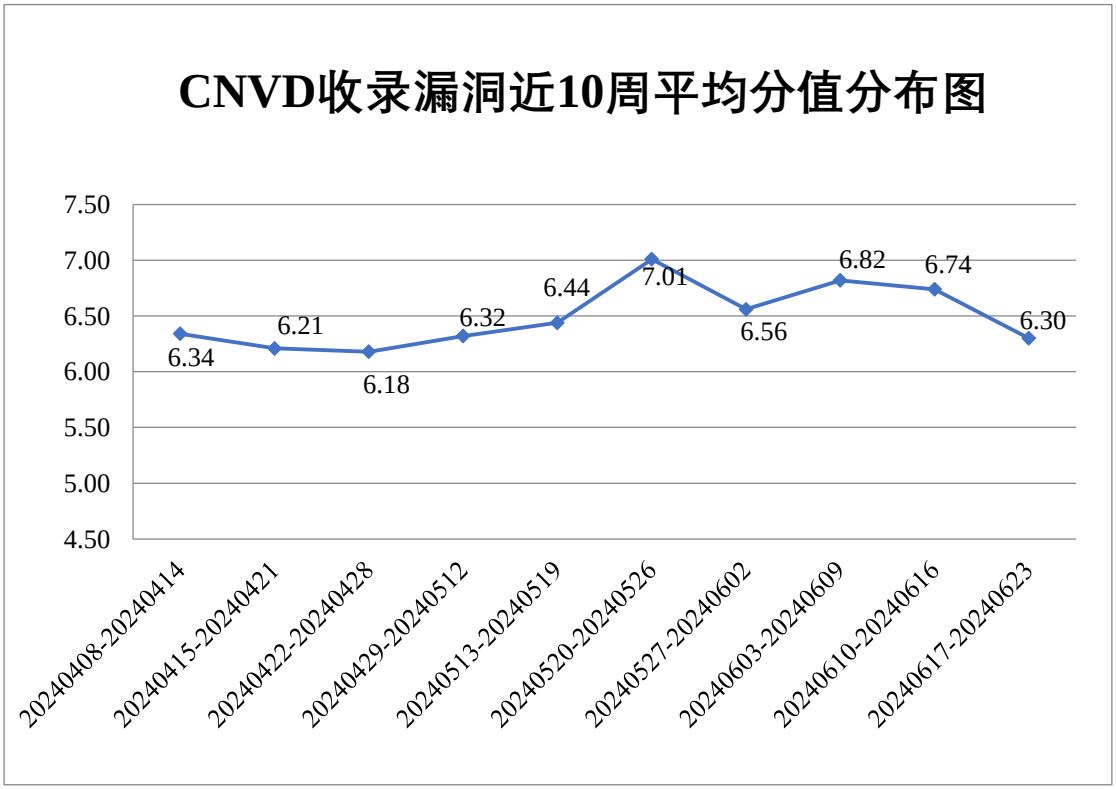

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 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 869 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 213 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 36 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：

重庆金鑫科技产业发展有限公司、中交智运有限公司、中国—东盟信息港股份有限公司、郑州千马企业管理咨询有限公司、浙江好络维医疗技术有限公司、浙江大华技术股份有限公司、长沙超级赏科技有限公司、枣庄市民卡管理有限公司、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、小米科技有限责任公司、西安字节音图电子科技有限公司、微软（中国）有限公司、统一通信（苏州）有限公司、天智（苏州）智能系统有限公司、天津市康婷生物工程集团有限公司、天津凤羽麟趾科技发展有限公司、索尼（中国）有限公司、松立控股集团股份有限公司、深圳市征铭科技有限公司、深圳市微耕实业有限公司、深圳市思源计算机软件股份有限公司、深圳市理昌智能科技有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市鼎游信息技术有限公司、深圳市必联电子有限公司、上海云翌通信科技有限公司、上海三高计算机中心股份有限公司、上海骐尘软件有限公司、上海蓝矩信息科技有限公司、上海电音马兰士电子有限公司、陕西瑞亚智能技术有限公司、山东潍微科技股份有限公司、厦门科拓通讯技术股份有限公司、赛蓝（广州）信息技术有限公司、融智通信息科技（天津）有限公司、青岛三利集团有限公司、青岛海信网络科技股份有限公司、奇瑞新能源汽车股份有限公司、普联技术有限公司、跑象科技（北京）有限公司、南京凌速科技有限公司、南京爱普雷德电子科技有限公司、马鞍山市创文通讯设备销售有限公司、马鞍山钱成似锦电子商务有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、连恩智能科技（上海）有限公司、柯尼卡美能达集团、京源中科科技股份有限公司、江苏三恒科技股份有限公司、佳能（中国）有限公司、华硕电脑（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、宏脉信息技术（广州）股份有限公司、杭州辛蜂网络科技有限公司、杭州海康威视数字技术股份有限公司、海南炎林网络科技有限公司、广州图创计算机软件开发有限公司、广州同鑫科技有限公司、广东飞企互联科技股份有限公司、固德威技术股份有限公司、富士施乐（中国）有限公司、福建科立讯通信有限公司、福建福昕软件开发股份有限公司、成都中科大旗软件股份有限公司、成都零起飞科技有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、禅道软件（青岛）有限公司、岑溪潮玩信息技术有限公司、北京中科聚网信息技术有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京神州视翰科技有限

公司、北京勤云科技发展有限公司、北京恰维网络科技有限公司、北京久其软件股份有限公司、北京百卓网络技术有限公司、安元科技股份有限公司、安徽科迅教育装备集团有限公司、The Apache Software Foundation、seacms、KYOCERA、Google 和 Adobe。

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、安天科技集团股份有限公司、北京天融信网络安全技术有限公司、杭州安恒信息技术股份有限公司、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、重庆都会信息科技有限公司、成都久信信息技术股份有限公司、北京山石网科信息技术有限公司、河南东方云盾信息技术有限公司、北京中睿天下信息技术有限公司、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、成都思维世纪科技有限责任公司、山石网科通信技术股份有限公司、华信咨询设计研究院有限公司、江苏极元信息技术有限公司、河南宝通信息安全测评有限公司、北方实验室（沈阳）股份有限公司、四川奇安旌服科技有限公司、江苏锋刃信息科技有限公司、西藏闪锁网络科技有限公司、中孚安全技术有限公司、深圳昂楷科技有限公司、北京翰慧投资咨询有限公司、信息产业信息安全测评中心、北京天防安全科技有限公司、北京神州泰岳软件股份有限公司、江苏百达智慧网络科技有限公司（含光实验室）、马鞍山书拓安全科技有限公司、江西中和证信息安全技术有限公司、成方金融科技有限公司上海分公司、北京时代新威信息技术有限公司、安徽天行网安信息安全技术有限公司、四川电科宏安科技有限公司、北京天下信安技术有限公司、上海亿保健康科技集团有限公司、南京聚铭网络科技有限公司、上海谋乐网络科技有限公司、厦门聚丁科技有限公司、吉林省吉林祥云信息技术有限公司、安徽赋能信息安全有限责任公司、湖南泛联新安信息科技有限公司、联通数字科技有限公司、江苏网擎信息技术有限公司、中国电信股份有限公司上海研究院、上海嘉韦思信息技术有限公司、中资网络信息安全科技有限公司、南方电网数字电网集团信息通信科技有限公司及其他个人白帽子向 CNVD 提交了 14284 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 12336 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）	8101	8101
奇安信网神（补天平台）	2451	2451
三六零数字安全科技	1420	1420

集团有限公司		
新华三技术有限公司	831	0
安天科技集团股份有限公司	596	0
北京天融信网络安全技术有限公司	590	11
上海交大	364	364
远江盛邦（北京）网络安全科技股份有限公司	184	184
杭州安恒信息技术股份有限公司	131	107
华为技术有限公司	129	1
恒安嘉新（北京）科技股份公司	106	0
北京长亭科技有限公司	99	1
深信服科技股份有限公司	98	98
北京启明星辰信息安全技术有限公司	70	4
京东科技信息技术有限公司	53	0
北京知道创宇信息技术有限公司	48	1
北京数字观星科技有限公司	26	0
北京安信天行科技有限公司	18	18
北京升鑫网络科技有限公司（青藤云）	14	14
杭州迪普科技股份有限公司	12	2
北京智游网安科技有限公司	5	5

北京神州绿盟科技有限公司	4	4
中国电信股份有限公司网络安全产品运营中心	1	1
江苏金盾检测技术股份有限公司	74	74
快页信息技术有限公司	74	74
重庆都会信息科技有限公司	61	61
成都久信信息技术股份有限公司	22	22
北京山石网科信息技术有限公司	21	21
河南东方云盾信息技术有限公司	19	19
北京中睿天下信息技术有限公司	9	9
苏州棱镜七彩信息科技有限公司	6	6
江苏晟晖信息科技有限公司	5	5
成都思维世纪科技有限责任公司	5	5
山石网科通信技术股份有限公司	5	5
华信咨询设计研究院有限公司	4	4
江苏极元信息技术有限公司	4	4
河南宝通信息安全测评有限公司	4	4
北方实验室（沈阳）股份有限公司	3	3

四川奇安旌服科技有限公司	3	3
江苏锋刃信息科技有限公司	3	3
西藏闪锁网络科技有限公司	3	3
中孚安全技术有限公司	3	3
深圳昂楷科技有限公司	3	3
北京翰慧投资咨询有限公司	3	3
信息产业信息安全测评中心	3	3
北京天防安全科技有限公司	2	2
北京神州泰岳软件股份有限公司	2	2
江苏百达智慧网络科技有限公司（含光实验室）	2	2
马鞍山书拓安全科技有限公司	2	2
江西中和证信息安全技术有限公司	2	2
成方金融科技有限公司上海分公司	2	2
北京时代新威信息技术有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
四川电科宏安科技有限公司	1	1
北京天下信安技术有限公司	1	1

上海亿保健康科技集团有限公司	1	1
南京聚铭网络科技有限公司	1	1
上海谋乐网络科技有限公司	1	1
厦门聚丁科技有限公司	1	1
吉林省吉林祥云信息技术有限公司	1	1
安徽赋能信息安全有限责任公司	1	1
湖南泛联新安信息科技有限公司	1	1
联通数字科技有限公司	1	1
江苏网擎信息技术有限公司	1	1
中国电信股份有限公司上海研究院	1	1
上海嘉韦思信息技术有限公司	1	1
中资网络信息安全科技有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
CNCERT 贵州分中心	2	2
个人	1127	1127
报送总计	16848	14284

本周漏洞按类型和厂商统计

本周，CNVD 收录了 314 个漏洞。按类型划分包括 WEB 应用 138 个，应用程序 96 个，网络设备（交换机、路由器等网络端设备）37 个，智能设备（物联网终端设备）

22 个，操作系统 13 个，数据库 7 个，安全产品 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	138
应用程序	96
网络设备（交换机、路由器等网络端设备）	37
智能设备（物联网终端设备）	22
操作系统	13
数据库	7
安全产品	1

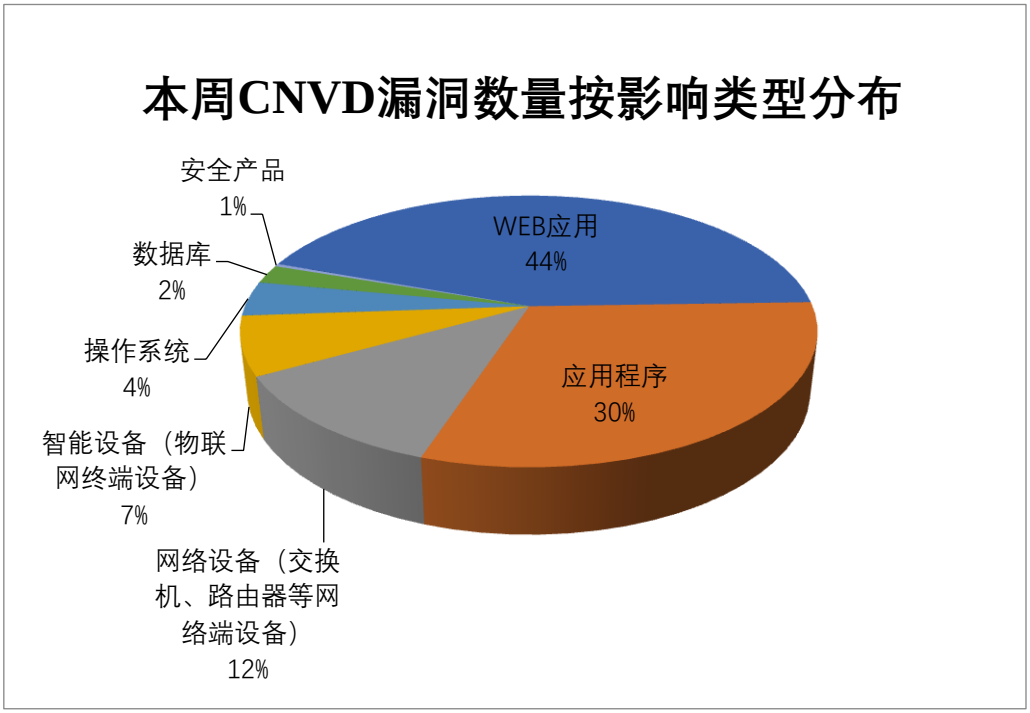

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、Siemens 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	52	16%
2	Google	16	5%
3	Siemens	11	4%
4	北京百卓网络技术有限公司	10	3%
5	SuiteCRM	9	3%
6	Apache	9	3%

7	北京星网锐捷网络技术有限公司	9	3%
8	Intelbras	6	2%
9	Linux	5	2%
10	其他	187	59%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，9 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2024-27515、CNVD-2024-27512）”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/

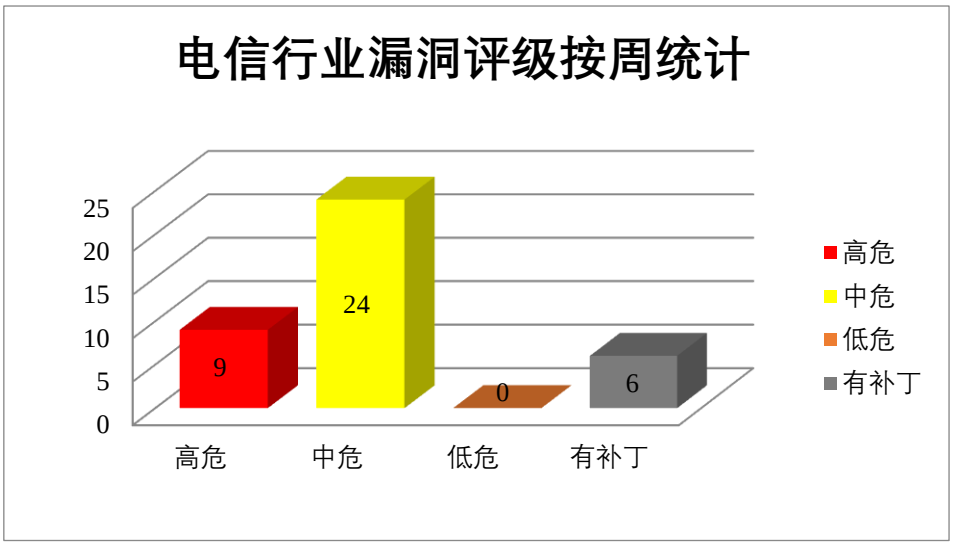

图 3 电信行业漏洞统计

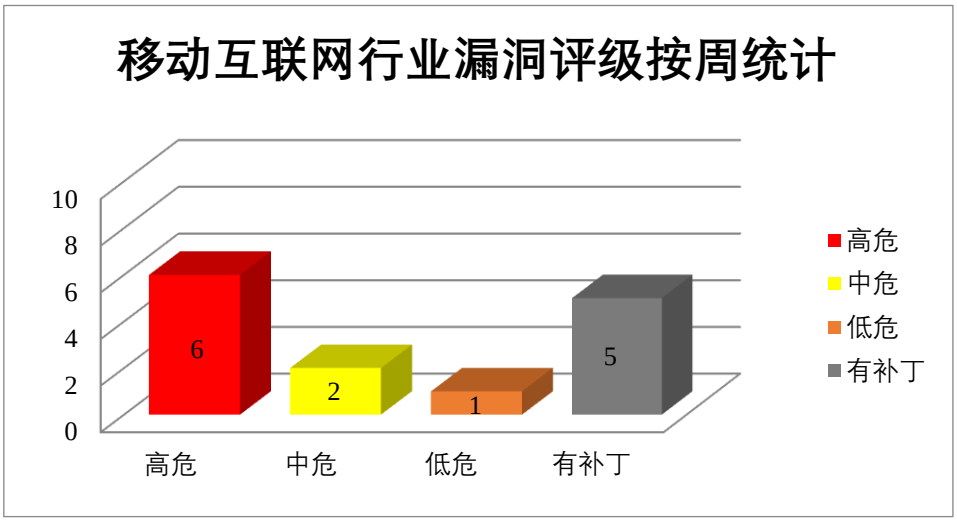

图 4 移动互联网行业漏洞统计

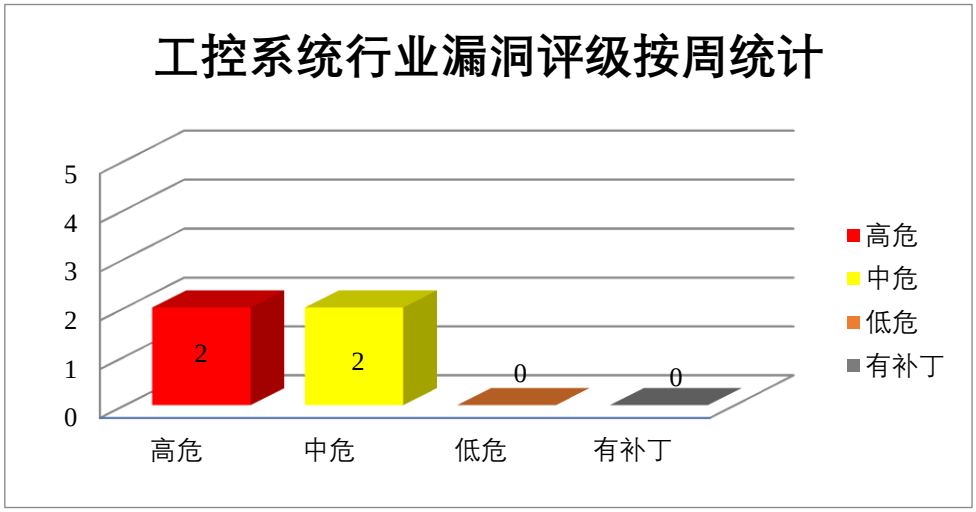

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。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，升级权限。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2024-27326、CNVD-2024-27323、CNVD-2024-27328）、Google Android 权限提升漏洞（CNVD-2024-27512、CNVD-2024-27513、CNVD-2024-27514、CNVD-2024-27515）、Google Android 信息泄露漏洞（CNVD-2024-27516）。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-2024-27326

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27323

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27328

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27512

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27513

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27514

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27515

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27516

2、 Apache 产品安全漏洞

Apache Sling 是美国阿帕奇（Apache）基金会的一个 Java 平台的开源 Web 框架。旨在在符合 JSR-170 的内容存储库（例如 Apache Jackrabbit）上创建以内容为中心的应用程序。Apache ActiveMQ 是美国阿帕奇（Apache）基金会的一套开源的消息中间件，它支持 Java 消息服务、集群、Spring Framework 等。Apache Arrow 是美国阿帕奇（Apache）基金会的一款用于内存数据处理的跨语言开发平台。该平台支持 C、C++、C＃、Go 和 Java 等编程语言，并提供进程间通信等功能。Apache DolphinScheduler 是美国阿帕奇（Apache）基金会的一个分布式的基于 DAG 可视化的工作流任务调度系统。Apache Axis 是美国阿帕奇（Apache）基金会的一个开源、基于 XML 的 Web 服务架构。该产品包含了 Java 和 C++语言实现的 SOAP 服务器，以及各种公用服务及 API，以生成和部署 Web 服务应用。Apache Ozone 是一个应用软件。一个面向 Hadoop 和云原生环境的可伸缩，冗余和分布式对象存储。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 ShenYu 是美国阿帕奇（Apache）基金会的一个异步的，高性能的，跨语言的，响应式的 API 网关。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使用特制的尾部标头造成反向代理走私，在未经身份验证的情况下载内部元数据，导致代码执行等。

CNVD 收录的相关漏洞包括：Apache Sling 路径遍历漏洞、Apache ActiveMQ 身份认证绕过漏洞、Apache Arrow 反序列化漏洞、Apache DolphinScheduler 输入验证错误漏洞（CNVD-2024-27495）、Apache Axis 代码问题漏洞、Apache Ozone 授权问题漏洞（CNVD-2024-27493）、Apache Tomcat 输入验证错误漏洞（CNVD-2024-27498）、Apache ShenYu 服务器端请求伪造漏洞。其中，除“Apache Ozone 授权问题漏洞（CNVD-2024-27493）、Apache Tomcat 输入验证错误漏洞（CNVD-2024-27498）、Apache ShenYu 服务器端请求伪造漏洞”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-2024-27492
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27491
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27496
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27495
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27494
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27493
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27498
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27497

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。Adobe Dreamweaver 是美国奥多比（Adobe）公司的一款基于 Windows 平台的支持可视化 HTML 编辑和代码编辑的软件。Adobe Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Aero 是美国奥多比（Adobe）公司的一款增强现实（AR）创作工具，它使用户能够利用平衡现实和虚拟现实技术，在现实世界中创建虚实结合的体验。Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。Adobe Substance 3D Designer 是美国奥多比（Adobe）公司的一款 3D 设计软件。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访问限制，获取敏感信息，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：Adobe Experience Manager 访问控制不当漏洞、Adobe Dreamweaver 操作系统命令注入漏洞、Adobe Framemaker 缓冲区溢出漏洞（CNVD-2024-27546）、Adobe Framemaker 堆缓冲区溢出漏洞（CNVD-2024-27545）、Adobe Aero 内存错误引用漏洞、Adobe Substance 3D Painter 越界写入漏洞（CNVD-2024-27549）、Adobe Substance 3D Designer 越界读取漏洞（CNVD-2024-27551）、Adobe Substance 3D Designer 越界写入漏洞（CNVD-2024-27552）。其中，除“Adobe Substance 3D Designer 越界读取漏洞（CNVD-2024-27551）”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-2024-27541
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27544
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27546
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27545
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27548
https://www.cnvd.org.cn/flaw/show/CNVD-2024-27549

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27551

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27552

4、Siemens 产品安全漏洞

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。Siemens SINEC NMS 是德国西门子（Siemens）公司的一个网络管理系统(NMS)，该系统可用于全天候集中监控、管理和配置具有数万台设备的工业网络，包括与安全相关的领域。Parasolild Translators 是单格式翻译器工具包，用于 Parasolid 和几种行业格式（如 STEP 或 IGES）之间的高速端到端翻译。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞覆盖任意文件，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens RUGGEDCOM CROSSBOW 信息泄露漏洞、Siemens RUGGEDCOM CROSSBOW 路径遍历漏洞、Siemens RUGGEDCOM CROSS BOW 缺少关键功能身份验证漏洞、Siemens SINEC NMS 路径遍历漏洞（CNVD-2024-27532）、Siemens PS/IGES Parasolid Translator 组件越界读取漏洞（CNVD-2024-27522）、Siemens PS/IGES Parasolid Translator 组件越界读取漏洞（CNVD-2024-27523、CNVD-2024-27524）、Siemens PS/IGES Parasolid Translator 组件类型混淆漏洞（CNVD-2024-27525）。其中，除“Siemens RUGGEDCOM CROSSBOW 信息泄露漏洞”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-2024-27526

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27527

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27531

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27532

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27522

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27523

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27524

https://www.cnvd.org.cn/flaw/show/CNVD-2024-27525

5、TOTOLINK EX1800T setRebootScheCfg 接口命令执行漏洞

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 被披露存在命令注入漏洞。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-2024-27559

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-2024-27325	Google Chrome 代码执行漏洞（CNVD-2024-27325）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop.html
CNVD-2024-27496	Apache Arrow 反序列化漏洞	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/yhy7tdfjf9hrl9vfrtzo8p2cyjq87v7n
CNVD-2024-27514	Google Android 权限提升漏洞（CNVD-2024-27514）	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/2024-05-01
CNVD-2024-27529	Siemens RUGGEDCOM CROSSBOW 文件名或路径外部控制漏洞（CNVD-2024-27529）	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-916916.html
CNVD-2024-27545	Adobe Framemaker 堆缓冲区溢出漏洞（CNVD-2024-27545）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/framemaker/apsb24-37.html
CNVD-2024-27560	FFmpeg 缓冲区溢出漏洞（CNVD-2024-27560）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10749
CNVD-2024-28191	SuiteCRM 路径遍历漏洞（CNVD-2024-28191）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/salesagility/SuiteCRM/releases/tag/v7.14.2
CNVD-2024-27332	Google Chrome 代码执行漏洞（CNVD-2024-27332）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop.html
CNVD-2024-27563	FFmpeg 缓冲区溢出漏洞（CNVD-2024-27563）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10758
CNVD-2024-28515	SuiteCRM 反序列化漏洞（CNVD-2024-28515）	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://docs.suitecrm.com/

小结：本周，Google 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，升级权限。此外，Apache、Adobe、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过访问限制，获取敏感信息，覆盖任意文件，执行任意代码，或导致应用程序崩溃等。另外，TOTOLINK EX1800T 被披露存在命令注入漏洞。攻击者可利用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、J2EEFAST BpmTaskFromMapper.xml 文件 SQL 注入漏洞

验证描述

J2eeFAST 是一个 Java EE 企业级快速开发平台， 致力于打造中小企业最好用的开源免费的后台框架平台。

J2EEFAST v2.7.0 版本存在 SQL 注入漏洞，该漏洞源于 BpmTaskFromMapper.xml 中的 findPage 函数缺少对外部输入 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/cxcxcxcxcxcxcxc/cxcxcxcxcxcxcxc/blob/main/cxcxcxcxcxc/about-2024/35086.txt

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-27555

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. Phoenix UEFI 固件曝出安全漏洞，数百款英特尔 PC 受影响

Phoenix SecureCore UEFI 固件中新发现一个漏洞被追踪为 CVE-2024-0762，该漏洞会影响运行多种英特尔 CPU 的设备，目前联想已经发布了新的固件更新以解决该漏洞。

参考链接：https://www.freebuf.com/news/404073.html

2. 华硕曝出安全漏洞，影响 7 款路由器

近期，华硕七种型号路由器曝出安全漏洞，漏洞被跟踪为 CVE-2024-3080（CVSS

v3.1 评分：9.8“严重”），是一个身份验证绕过漏洞，允许未经身份验证的远程威胁攻击者控制设备。华硕方面在发布的固件更新中解决了安全漏洞问题。

参考链接：https://www.freebuf.com/news/403718.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