国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 06 月 05 日-2023 年 06 月 11 日 **2023 年第 23 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**高**。

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 254 个，其中高危漏洞 175 个、中危漏洞 68 个、低危漏洞 11 个。漏洞平均分值为 7.24。本周收录的漏洞中，涉及 0day 漏洞 206 个（占 81%），其中互联网上出现“Tenda AC23 命令注入漏洞、Faculty Evaluation System SQL 注入漏洞（CNVD-2023-45448）”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 27201 个，与上周（12598 个）环比增加 1.16 倍。

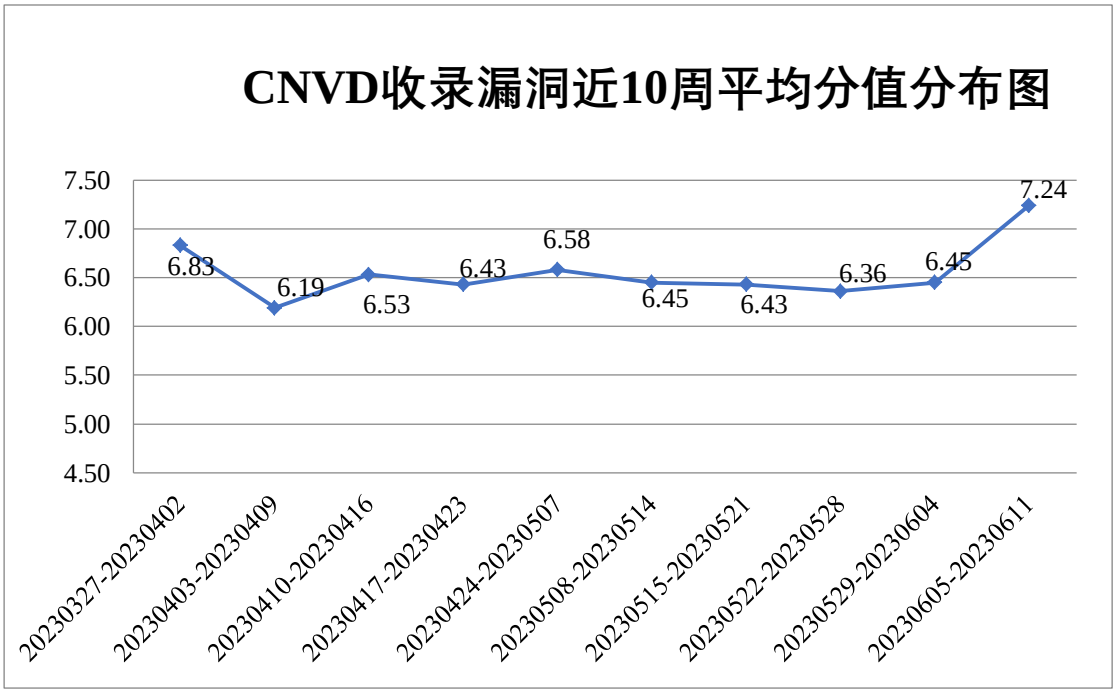

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 起，向基础电

信企业通报漏洞事件 24 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 805 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 200 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 59 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：

珠海经济特区伟思有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆风速信息科技有限公司、众惠其珹商城有限公司、中兴保全科技股份有限公司、中金亚洲（北京）国际互联网科技有限公司、郑州众智科技股份有限公司、郑州天迈科技股份有限公司、郑州三和水工机械有限公司、浙江码尚科技股份有限公司、浙江兰德纵横网络技术股份有限公司、浙江大华技术股份有限公司、浙江爱充网络科技有限公司、掌如科技服务有限公司、长沙米拓信息技术有限公司、云易宿（北京）文旅科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易迅通科技有限公司、易家健康管理有限公司、襄阳软宝信息科技有限公司、西安点测网络科技有限公司、武汉城投停车场投资建设管理有限公司、统信软件技术有限公司、同方知网（北京）技术有限公司、四平市九州易通科技有限公司、四创科技有限公司、四川易泊时捷智能科技有限公司、四川易迪优信息技术有限公司、神州数码控股有限公司、深圳维盟科技股份有限公司、深圳市信维通信股份有限公司、深圳市西迪特科技股份有限公司、深圳市网心科技有限公司、深圳市四海众联网络科技有限公司、深圳市联软科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市慧为智能科技股份有限公司、深圳市道尔智控科技股份有限公司、深圳市触拓科技有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、深圳科士达科技股份有限公司、深圳华视美达信息技术有限公司、申瓯通信设备有限公司 、上汽红岩汽车有限公司 、上海卓卓网络科技有限公司、上海真兰仪表科技股份有限公司、上海叶渺生物科技中心、上海唯善科技有限公司、上海淘满家电子商务有限公司、上海清美新鲜到家网络科技有限公司、上海米健信息技术有限公司、上海肯特仪表股份有限公司、上海金电网安科技有限公司、上海酆泽信息技术有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海贝锐信息科技股份有限公司、上海爱数信息技术股份有限公司、商丘芝麻开门网络科技有限公司、商派软件有限公司、山西豆蔻文化传播有限公司、山西大禹生物工程股份有限公司、山东开创集团股份有限公司、山东京帝软件有限公司、山东广安车联科技股份有限公司、厦门市灵鹿谷科技有限公司、厦门狮子鱼网络科技有限公司、瑞鑫点教（北京）科技有限公司、日立（中国）有限公司、全天数据管理有限公司、青岛培诺教育科技股份有限公司、青岛百洋健康药房连锁有限公司、侨益物流股份有限公司、麒麟软件有限公司、邳州天目网络科技有限公司、南京矽汇信息技术有限公司、民力建设咨询集团有限公司、蛮牛健康管理服务有限公司、龙采科技集团有限责任公司、灵宝简好网络科技

有限公司、理光（中国）投资有限公司、联想（北京）有限公司、浪潮通用软件有限公司、康桥悦生活服务集团有限公司、康博嘉信息科技（北京）股份有限公司、巨迈网络科技有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、江苏万林现代物流股份有限公司、江苏叁拾叁信息技术有限公司、江苏金智教育信息股份有限公司、江苏好润生物科技有限公司、佳能（中国）有限公司、济宁云课网络科技有限公司、济南智学酷教育科技有限公司、技嘉科技股份有限公司、吉翁电子（深圳）有限公司、积成电子股份有限公司、混沌时代（北京）教育科技有限公司、惠普贸易（上海）有限公司、湖南心诺科技集团有限公司、湖南省新华书店有限责任公司、湖南强智科技发展有限公司、湖北点点点科技有限公司、河北鑫众博教育科技有限公司、合肥盛东信息科技有限公司、杭州先锋电子技术股份有限公司、杭州来疯科技有限公司、杭州大搜车汽车服务有限公司、哈尔滨伟成科技有限公司、国信云联数据科技股份有限公司、广州粤建三和软件股份有限公司、广州图创计算机软件开发有限公司、广州同福信息科技有限公司、广州市玄武无线科技股份有限公司、广州市超易信息科技有限公司、广州青鹿教育科技有限公司、广州科天视畅信息科技有限公司、广州金博信息技术有限公司、广东雪域藏药连锁有限公司、广东万和新电气股份有限公司、多伦科技股份有限公司、东华医为科技有限公司、东华软件股份公司、帝国软件、当代教育科技集团有限公司、辰安云服技术有限公司、畅畅行网络科技有限公司、北京中科金马科技股份有限公司、北京致远互联软件股份有限公司、北京泽元迅长软件有限公司、北京易金卡网络技术有限公司、北京学大信息技术集团有限公司、北京星网锐捷网络技术有限公司、北京小桔科技有限公司、北京文华在线教育科技股份有限公司、北京网康科技有限公司、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、北京巧巧时代网络科技有限公司、北京凯特伟业科技有限公司、北京卡车之家信息技术股份有限公司、北京宏景世纪软件股份有限公司、北京国尚信科技有限公司、北京高知图新教育科技有限公司、北京春雨天下软件有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安徽中技国医医疗科技有限公司、安徽青柿信息科技有限公司、ZZCMS、QEMU、LuckyFrame、Kyland Technology Co., Ltd 和 Electronics For Imaging, Inc。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，远江盛邦（北京）网络安全科技股份有限公司、深信服科技股份有限公司、新华三技术有限公司、安天科技集团股份有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。快页信息技术有限公司、上海齐同信息科技有限公司、杭州美创科技有限公司、重庆电信系统集成公司、河南东方云盾信息技术有限公司、北京升鑫网络科技有限公司、河南信安世纪科技有限公司、北京赛博昆仑科技有限公司、贵州多彩网安科技有限公司、联想集团、北京众安

天下科技有限公司、河北锐远网络科技有限公司、中国电信股份有限公司上海研究院、成都思维世纪科技有限责任公司、山东新潮信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、山东鼎夏智能科技有限公司、上海纽盾科技股份有限公司、赛尔网络有限公司、海南大学、北京华云安信息技术有限公司、广州安亿信软件科技有限公司、江苏君立华域信息安全技术股份有限公司、重庆易阅科技有限公司、超聚变数字技术有限公司、信息产业信息安全测评中心、北京山石网科信息技术有限公司、内蒙古洞明科技有限公司、软通动力信息技术（集团）股份有限公司、河南省鼎信信息安全等级测评有限公司、郑州埃文科技、深圳市智安网络有限公司、北京珞安科技有限责任公司、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 27201 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 24158 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
奇安信网神（补天平台）	21996	21996
三六零数字安全科技集团有限公司	873	873
上海交大	708	708
斗象科技（漏洞盒子）	581	581
远江盛邦（北京）网络安全科技股份有限公司	430	430
深信服科技股份有限公司	405	9
新华三技术有限公司	393	0
安天科技集团股份有限公司	310	0
北京启明星辰信息安全技术有限公司	300	0
北京天融信网络安全技术有限公司	181	3
北京神州绿盟科技有限公司	153	5
阿里云计算有限公司	130	1
北京数字观星科技有	78	0

限公司		
北京长亭科技有限公司	60	16
天津市国瑞数码安全系统股份有限公司	59	0
京东科技信息技术有限公司	19	1
中国电信集团系统集成有限责任公司	17	0
杭州迪普科技股份有限公司	14	0
杭州安恒信息技术股份有限公司	11	2
北京智游网安科技有限公司	2	2
北京知道创宇信息技术有限公司	1	0
卫士通信息产业股份有限公司	1	1
浙江大华技术股份有限公司	1	1
北京信联数安科技有限公司	1	1
快页信息技术有限公司	134	134
上海齐同信息科技有限公司	72	72
杭州美创科技有限公司	51	51
重庆电信系统集成公司	46	46
河南东方云盾信息技术有限公司	36	36
北京升鑫网络科技有限公司	28	28

河南信安世纪科技有限公司	27	27
北京赛博昆仑科技有限公司	25	25
贵州多彩网安科技有限公司	19	19
联想集团	16	16
北京众安天下科技有限公司	14	14
河北镌远网络科技有限公司	13	13
中国电信股份有限公司上海研究院	11	11
成都思维世纪科技有限责任公司	10	10
山东新潮信息技术有限公司	5	5
北京云科安信科技有限公司（Seraph 安全实验室）	5	5
山东鼎夏智能科技有限公司	4	4
上海纽盾科技股份有限公司	4	4
赛尔网络有限公司	3	3
海南大学	2	2
北京华云安信息技术有限公司	2	2
广州安亿信软件科技有限公司	2	2
江苏君立华域信息安全技术股份有限公司	2	2
重庆易阅科技有限公司	2	2
超聚变数字技术有限	2	2

公司		
信息产业信息安全测评中心	2	2
北京山石网科信息技术有限公司	1	1
内蒙古洞明科技有限公司	1	1
软通动力信息技术（集团）股份有限公司	1	1
河南省鼎信信息安全等级测评有限公司	1	1
郑州埃文科技	1	1
深圳市智安网络有限公司	1	1
北京珞安科技有限责任公司	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 河北分中心	6	6
CNCERT 广西分中心	6	6
CNCERT 贵州分中心	2	2
CNCERT 陕西分中心	1	1
个人	2011	2011
报送总计	29295	27201

本周漏洞按类型和厂商统计

本周，CNVD 收录了 254 个漏洞。WEB 应用 162 个，应用程序 40 个，网络设备（交换机、路由器等网络端设备）31 个，操作系统 15 个，智能设备（物联网终端设备）5 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	162
应用程序	40
网络设备（交换机、路由器等网络端设备）	31
操作系统	15
智能设备（物联网终端设备）	5
安全产品	1

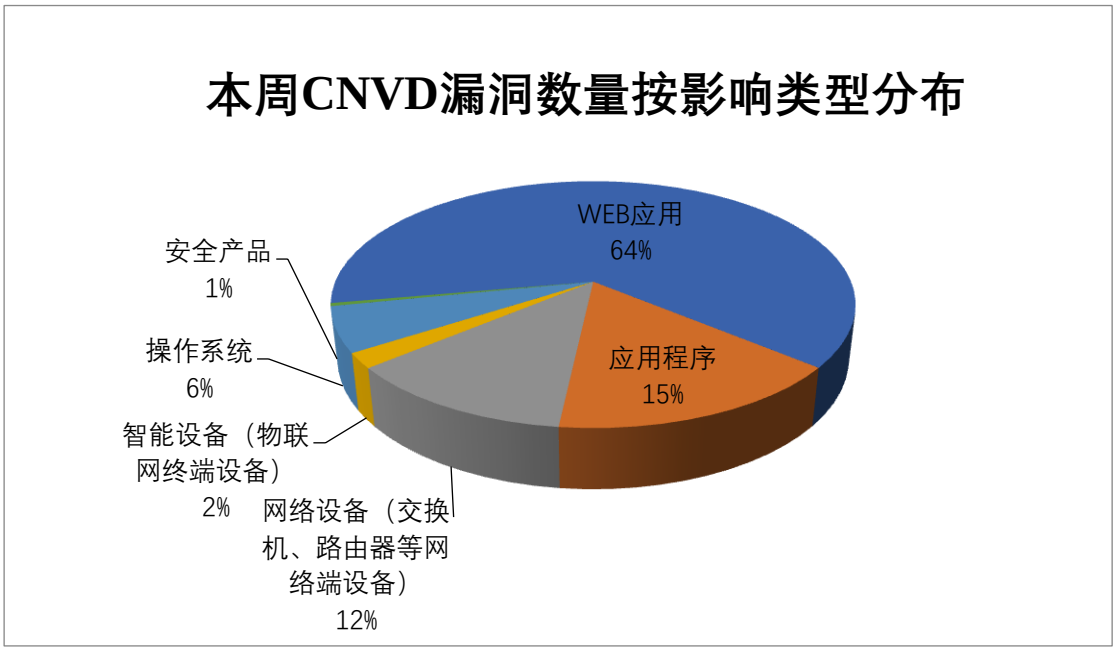

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、Rockwell Automation 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	Google	14	5%
2	Adobe	10	4%
3	Rockwell Automation	9	4%
4	Microsoft	8	3%
5	新华三技术有限公司	6	2%
6	深圳市必联电子有限公司	5	2%
7	北京网康科技有限公司	4	2%
8	Laundry Booking Management System	4	2%
9	Tenda	4	2%
10	其他	190	74%

本周行业漏洞收录情况

本周，CNVD 收录了 28 个电信行业漏洞，12 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，“Hitron Technologies CODA-5310 远程命令执行漏洞、Rockwell Automation ArmorStart ST 跨站脚本漏洞（CNVD-2023-44294）”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/

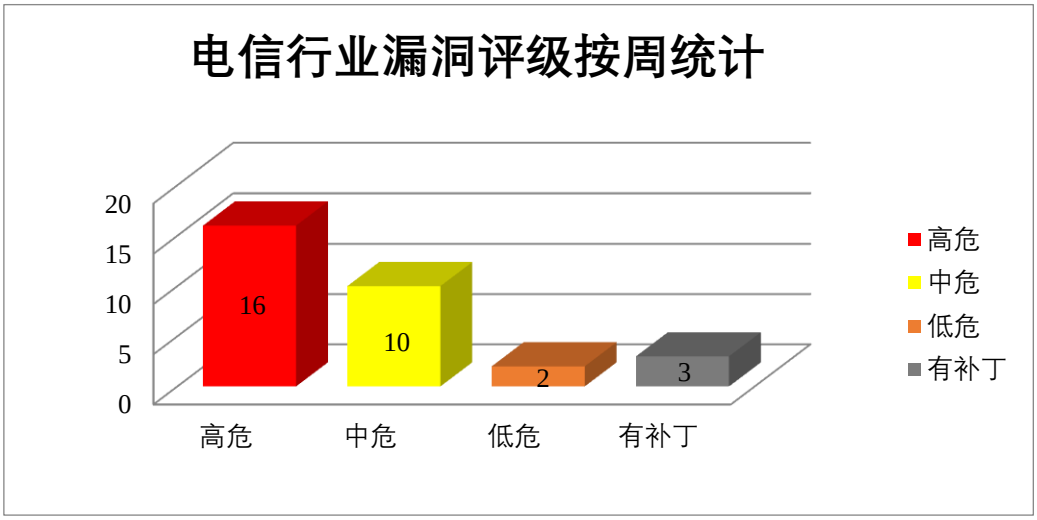

图 3 电信行业漏洞统计

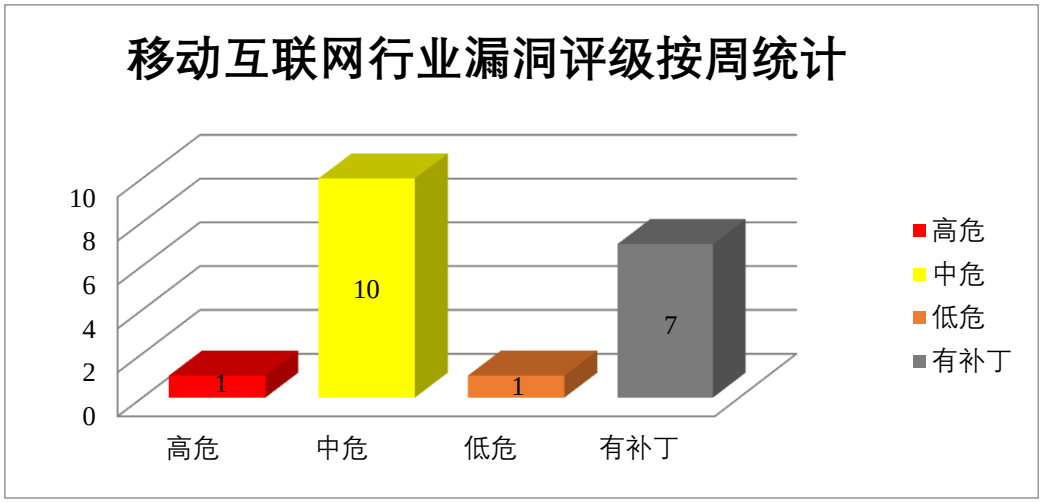

图 4 移动互联网行业漏洞统计

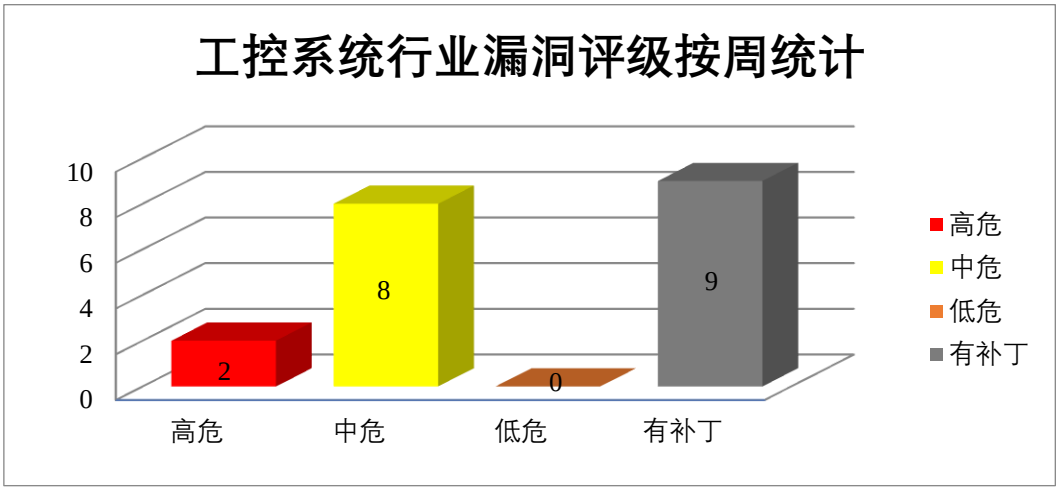

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Windows DNS 是美国微软（Microsoft）公司的一个域名解析服务。域名系统（DNS）是包含 TCP / IP 的行业标准协议套件之一，并且 DNS 客户端和 DNS 服务器共同为计算机和用户提供计算机名称到 IP 地址的映射名称解析服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致信息泄露，远程代码执行。

CNVD 收录的相关漏洞包括：Microsoft Windows DNS 远程代码执行漏洞（CNVD-2023-44299、CNVD-2023-44297、CNVD-2023-44298、CNVD-2023-44303、CNVD-2023-44302、CNVD-2023-44300、CNVD-2023-44304）、Microsoft Windows DNS 信息泄露漏洞。其中，除“Microsoft Windows DNS 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-2023-44299

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44298

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44297

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44303

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44302

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44301

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44300

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44304

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。Google Android

是一套以 Linux 为基础的开源操作系统。Google TensorFlow 是一套用于机器学习的端到端开源平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面潜在地利用堆损坏，导致内存损坏，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome Navigation 内存错误引用漏洞、Google Android 资源管理错误漏洞（CNVD-2023-43880）、Google Android 输入验证错误漏洞（CNVD-2023-43879）、Google Chrome 类型混淆漏洞（CNVD-2023-43877）、Google Chrome 缓冲区溢出漏洞（CNVD-2023-43887、CNVD-2023-43886、CNVD-2023-43885）、Google TensorFlow 缓冲区溢出漏洞（CNVD-2023-43888）。其中，除“Google Android 资源管理错误漏洞（CNVD-2023-43880）、Google Android 输入验证错误漏洞（CNVD-2023-43879）”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-2023-43876
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43880
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43879
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43877
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43887
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43886
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43885
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43888

3、Adobe 产品安全漏洞

Adobe Substance 3D Stager 是美国奥多比（Adobe）公司的一个虚拟 3D 工作室。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用户的上下文中执行代码。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Stager 堆缓冲区溢出漏洞（CNVD-2023-43891、CNVD-2023-43895）、Adobe Substance 3D Stager 越界写入漏洞（CNVD-2023-43897、CNVD-2023-43893）、Adobe Substance 3D Stager 内存错误引用漏洞、Adobe Substance 3D Stager 越界读取漏洞（CNVD-2023-43894、CNVD-2023-43899、CNVD-2023-43890）。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-2023-43891
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43890
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43893
https://www.cnvd.org.cn/flaw/show/CNVD-2023-43892

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43895

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43894

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43897

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43899

4、Rockwell Automation 产品安全漏洞

Rockwell Automation ArmorStart ST 是美国罗克韦尔（Rockwell Automation）公司的一种用于机旁控制架构的简单而经济实用的解决方案。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话，查看和修改敏感数据或使网页不可用等。

CNVD 收录的相关漏洞包括：Rockwell Automation ArmorStart ST 跨站脚本漏洞（CNVD-2023-44289、CNVD-2023-44288、CNVD-2023-44293、CNVD-2023-44292、CNVD-2023-44291、CNVD-2023-44290、CNVD-2023-44296、CNVD-2023-44295）。其中，“Rockwell Automation ArmorStart ST 跨站脚本漏洞（CNVD-2023-44292、CNVD-2023-44296）”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-2023-44289

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44288

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44293

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44292

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44291

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44290

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44296

https://www.cnvd.org.cn/flaw/show/CNVD-2023-44295

5、ASUS RT-AC86U 缓冲区溢出漏洞

ASUS RT-AC86U 是中国华硕（ASUS）公司的一款双频 Wi-Fi 路由器。本周，ASUS RT-AC86U 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞执行任意系统命令、中断系统或终止服务。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-2023-45450

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.htm

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-2023-43877	Google Chrome 类型混淆漏洞（CNVD-2023-43877）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_16.html
CNVD-2023-43885	Google Chrome 缓冲区溢出漏洞（CNVD-2023-43885）	高	厂商已发布了漏洞修复程序，请及时关注更新: https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html
CNVD-2023-43888	Google TensorFlow 缓冲区溢出漏洞（CNVD-2023-43888）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6hg6-5c2q-7rcr
CNVD-2023-43890	Adobe Substance 3D Stager 越界读取漏洞	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/substance3d_stager/apsb23-22.html
CNVD-2023-43896	Adobe Substance 3D Stager 不当输入验证漏洞	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/substance3d_stager/apsb23-22.html
CNVD-2023-43898	Adobe Substance 3D Stager 不当输入验证漏洞（CNVD-2023-43898）	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/substance3d_stager/apsb23-22.html
CNVD-2023-44292	Rockwell Automation Armor Start ST 跨站脚本漏洞（CNVD-2023-44292）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438
CNVD-2023-44297	Microsoft Windows DNS 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28308
CNVD-2023-45001	Nacos Jraft Hessian 反序列漏洞	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://github.com/alibaba/nacos/releases/tag/1.4.6 https://github.com/alibaba/nacos/releases/tag/2.2.3
CNVD-2023	Hitron Technologies CODA-5	高	厂商已发布了漏洞修复程序，请及

-45451	310 远程命令执行漏洞		时关注更新：https://www.hitrontech.com/zh-tw/products/coda-5310-cable-gateway/

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞导致信息泄露，远程代码执行。此外，Google、Adobe、Rockwell Automation 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行代码，导致内存损坏或造成拒绝服务等。另外，ASUS RT-AC86U 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞执行任意系统命令、中断系统或终止服务。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、Faculty Evaluation System SQL 注入漏洞（CNVD-2023-45448）

验证描述

Faculty Evaluation System 是一个教师评估系统。

Faculty Evaluation System 存在 SQL 注入漏洞，攻击者可利用该漏洞通过构造恶意查询语句来直接操作数据库，从而获取敏感信息或者执行任意的操作。

验证信息

POC 链接：https://github.com/F14me7wq/bug_report/blob/main/vendors/oretnom23/faculty-evaluation-system/SQLi-1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-45448

信息提供者

北京长亭科技有限公司

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. Visual Studio 漏洞值得警惕

Varonis 安全研究人员警告称，微软此前修复的一个 Visual Studio 安装程序漏洞危害不容小视，攻击者可以利用此漏洞伪装成合法的软件，创建和分发恶意扩展程序，对开发环境进行渗透，从而掌控代码、窃取高价值的知识产权。

参考链接：https://www.darkreading.com/application-security/researchers-warn-of-easily-exploitable-spoofing-bug-in-visual-studio

2. 思科和 VMware 解决安全漏洞

VMware 已发布安全更新，以修复 Aria Operations for Networks 中可能导致信息泄露和远程代码执行的三个缺陷。

参考链接：https://thehackernews.com/2023/06/urgent-security-updates-cisco-and.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