

信息安全漏洞周报

2023年07月31日-2023年08月06日

2023年第31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 396 个，其中高危漏洞 210 个、中危漏洞 172 个、低危漏洞 14 个。漏洞平均分为 6.69。本周收录的漏洞中，涉及 0day 漏洞 336 个（占 85%），其中互联网上出现“AdvanceMAME 堆栈缓冲区溢出漏洞、Milesight UR32L firewall_handler_set 函数缓冲区溢出漏洞（CNVD-2023-61192）”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 28470 个，与上周（30305 个）环比减少 6%。

CNVD收录漏洞近10周平均分分布图

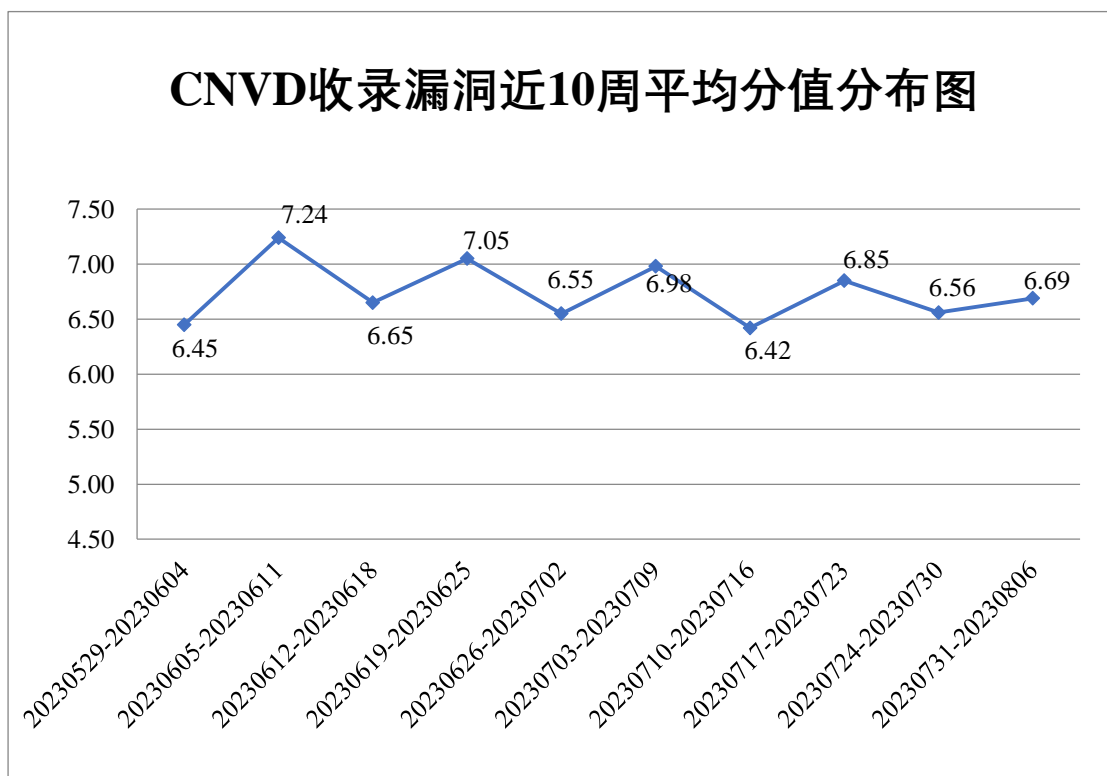


图 1 CNVD 收录漏洞近 10 周平均分分布图


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 15 起，向基础电信企业通报漏洞事件 6 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 914 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 185 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 28 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：

重庆中联信息产业有限责任公司、重庆小丢科技有限公司、重庆森鑫炬科技有限公司、中新网络信息安全股份有限公司、中科三清科技有限公司、中电鸿信信息科技有限公司、中安云科科技发展（山东）有限公司、郑州三晖电气股份有限公司、正方软件股份有限公司、浙江一鸣食品股份有限公司、浙江荣鹏气动工具股份有限公司、浙江吉利控股集团汽车销售有限公司、浙江大华技术股份有限公司、浙江苍南仪表集团股份有限公司、云南艾图内控规范研究院有限公司、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、银泰商业管理集团有限公司、亿米供应链管理有限公司、一重新能源发展集团有限公司、兄弟（中国）商业有限公司、信呼、新开普电子股份有限公司、武汉益模科技股份有限公司、武汉天地伟业科技有限公司、武汉盛科达科技有限公司、薇拉文化集团有限公司、天维尔信息科技股份有限公司、天津神州浩天科技有限公司、天际汽车科技集团有限公司、泰华智慧产业集团股份有限公司、泰禾集团股份有限公司、四川迅睿云软件开发有限公司、数字海南有限公司、圣奥科技股份有限公司、沈阳点动科技有限公司、神州数码集团股份有限公司、神彩科技股份有限公司、深圳市网心科技有限公司、深圳市天朗时代科技有限公司、深圳市锐明技术股份有限公司、深圳市萌爱动漫文化发展有限公司、深圳市吉祥腾达科技有限公司、深圳市博思协创网络科技有限公司、深圳市必联电子有限公司、深圳市拜特科技股份有限公司、深圳市安居宝电子有限公司、深圳前海微众银行股份有限公司、深圳齐心好视通云计算有限公司、深圳联友科技有限公司、深圳傲鸿科技有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海延华智能科技（集团）股份有限公司、上海卫宁数据科技有限公司、上海万物新生环保科技集团有限公司、上海荃路软件开发工作室、上海灵当信息科技有限公司、上海金榜智能科技有限公司、上海嘉扬信息系统有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、熵基科技股份有限公司、商派软件有限公司、山西牛之云网络科技有限公司、厦门市理臣教育服务有限公司、任子行网络技术股份有限公司、全美在线（北京）科技股份有限公司、青岛易软天创网络科技有限公司、普元信息技术股份有限公司、普联技术有限公司、南宁迈世信息技术有限公司、摩莎科技（上海）有限公司、梦想 CMS、迈普通信技术股份有限公司、隆基绿能

科技股份有限公司、浪潮通用软件有限公司、朗致集团有限公司、蓝盾信息安全技术有限公司、康泰克（上海）信息科技有限公司、卡莱特云科技股份有限公司、江苏紫清信息科技有限公司、江苏有线网络发展发展有限责任公司吴江分公司、江苏领悟信息技术有限公司、江苏安科瑞电器制造有限公司、济宁云课网络科技有限公司、吉翁电子（深圳）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、弘扬软件股份有限公司、河南易税科技有限公司、河南德力汽车销售有限公司、杭州雄伟科技开发股份有限公司、杭州新中大科技股份有限公司、杭州乐刻网络技术有限公司、杭州蓝代斯克数字技术有限公司、杭州阔知网络科技有限公司、杭州今奥信息科技股份有限公司、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、汉江智行科技有限公司、哈尔滨伟成科技有限公司、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、广州酷狗计算机科技有限公司、广州霸天安安防科技有限公司、广联达科技股份有限公司、广东优信无限网络股份有限公司、广东省健缘云健康管理有限公司、广东飞企互联科技股份有限公司、广东方天软件科技股份有限公司、广东东宏智控科技股份有限公司、高等教育电子音像出版社有限公司、富士胶片商业创新（中国）有限公司、福州联讯信息科技有限公司、福建卡卡智能电子科技有限公司、佛山市淇特科技有限公司、东莞市宇腾信息科技有限公司、大连华天软件有限公司、成都延华西部健康医疗信息产业研究院有限公司、成都索贝数码科技股份有限公司、成都芄博科技有限公司、畅捷通信息技术股份有限公司、布瑞克（苏州）农业互联网股份有限公司、北京众鸣世纪科技有限公司、北京印象笔记科技有限公司、北京星网锐捷网络技术有限公司、北京鑫丰南格科技股份有限公司、北京小桔科技有限公司、北京西控电子商务有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京搜精品经贸有限公司、北京猎鹰安全科技有限公司、北京朗新天霁软件技术有限公司、北京快松果科技有限公司、北京久其软件股份有限公司、北京金和网络股份有限公司、北京慧飒科技有限责任公司、北京鸿旭文化发展集团有限公司、北京点趣教育科技有限公司、北京百卓网络技术有限公司、北奔重型汽车集团有限公司、安徽商信政通信息技术股份有限公司、爱普生（中国）有限公司、鼎捷软件股份有限公司、ZZCMS、WAVLINK、taoCMS、semcms、PowerJob、nginxWEBUI、kettle 管理平台、Joomla 和 HadSky。



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、新华三技术有限公司、安天科技集团股份有限公司、北京数字观星科技有限公司、杭州安恒信息技术股份有限公司等单位报送公开收集的漏洞数量较多。杭州美创科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、联想集团、安徽锋刃信息科技有限公司、重庆电信系统集成有限公司、快页信息技术有限公司、河南信安世纪科技有限公司、亚信科技（成都）

有限公司、河南东方云盾信息技术有限公司、河北镌远网络科技有限公司、信息产业信息安全测评中心、赛尔网络有限公司、卫士通（广州）信息技术有限公司、星云博创科技有限公司、北京山石网科信息技术有限公司、广州安亿信软件科技有限公司、杭州默安科技有限公司、南京聚铭网络科技有限公司、杭州捷鼎科技有限公司、北京水木羽林科技有限公司、河南省鼎信信息安全等级测评有限公司、南京深安科技有限公司、西藏熙安信息技术有限责任公司、软通动力信息技术（集团）股份有限公司、安徽思珀特信息科技有限公司、北京华顺信安信息技术有限公司、智网安云（武汉）信息技术有限公司、上海纽盾科技股份有限公司、北京赛博昆仑科技有限公司、成都安美勤信息技术股份有限公司、北京君云天下科技有限公司、江苏晟晖信息科技有限公司、山东九域信息技术有限公司、北京安帝科技有限公司、中国电信股份有限公司上海研究院、云卫士（福建）科技有限公司、江苏保旺达软件技术有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 28470 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、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 26232 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）	17232	17232
斗象科技（漏洞盒子）	7431	7431
三六零数字安全科技集团有限公司	847	847
上海交大	722	722
深信服科技股份有限公司	565	0
新华三技术有限公司	338	0
安天科技集团股份有限公司	320	0
北京数字观星科技有限公司	220	0
杭州安恒信息技术股份有限公司	212	212
北京启明星辰信息安全技术有限公司	122	43
阿里云计算有限公司	99	1
北京长亭科技有限公	82	7

司		
北京知道创宇信息技术有限公司	75	1
天津市国瑞数码安全系统股份有限公司	59	0
远江盛邦（北京）网络安全科技股份有限公司	52	52
杭州迪普科技股份有限公司	33	0
南京众智维信息科技有限公司	29	29
京东科技信息技术有限公司	7	7
西安四叶草信息技术有限公司	4	4
北京天融信网络安全技术有限公司	3	3
北京信联数安科技有限公司	1	1
北京神州绿盟科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
杭州美创科技有限公司	120	120
奇安星城网络安全运营服务（长沙）有限公司	57	57
联想集团	50	50
安徽锋刃信息科技有限公司	49	49
重庆电信系统集成有限公司	34	34

快页信息技术有限公司	20	20
河南信安世纪科技有限公司	16	16
亚信科技（成都）有限公司	13	13
河南东方云盾信息技术有限公司	8	8
河北铸远网络科技有限公司	7	7
信息产业信息安全测评中心	7	7
赛尔网络有限公司	7	7
卫士通（广州）信息安全技术有限公司	6	6
星云博创科技有限公司	6	6
北京山石网科信息技术有限公司	5	5
广州安亿信软件科技有限公司	4	4
杭州默安科技有限公司	3	3
南京聚铭网络科技有限公司	3	3
杭州捷鼎科技有限公司	3	3
北京水木羽林科技有限公司	3	3
任子行网络技术股份有限公司	2	2
河南省鼎信信息安全等级测评有限公司	2	2
南京深安科技有限公司	2	2

西藏熙安信息技术有 限责任公司	2	2
软通动力信息技术 (集团) 股份有限公 司	2	2
安徽思珀特信息科技 有限公司	2	2
北京华顺信安信息技 术有限公司	1	1
智网安云(武汉)信 息技术有限公司	1	1
上海纽盾科技股份有 限公司	1	1
北京赛博昆仑科技有 限公司	1	1
成都安美勤信息技术 股份有限公司	1	1
北京君云天下科技有 限公司	1	1
江苏晟晖信息科技有 限公司	1	1
山东九域信息技术有 限公司	1	1
北京安帝科技有限公 司	1	1
中国电信股份有限公 司上海研究院	1	1
云卫士(福建)科技 有限公司	1	1
江苏保旺达软件技术 有限公司	1	1
CNCERT 广西分中心	15	15
CNCERT 贵州分中心	4	4
CNCERT 河北分中心	3	3
个人	1409	1409

报送总计	30331	28470
------	-------	-------

本周漏洞按类型和厂商统计

本周，CNVD 收录了 396 个漏洞。WEB 应用 230 个，应用程序 78 个，网络设备（交换机、路由器等网络端设备）60 个，操作系统 14 个，安全产品 6 个，智能设备（物联网终端设备）4 个，数据库 3 个，车联网 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	230
应用程序	78
网络设备（交换机、路由器等网络端设备）	60
操作系统	14
安全产品	6
智能设备（物联网终端设备）	4
数据库	3
车联网	1

本周CNVD漏洞数量按影响类型分布

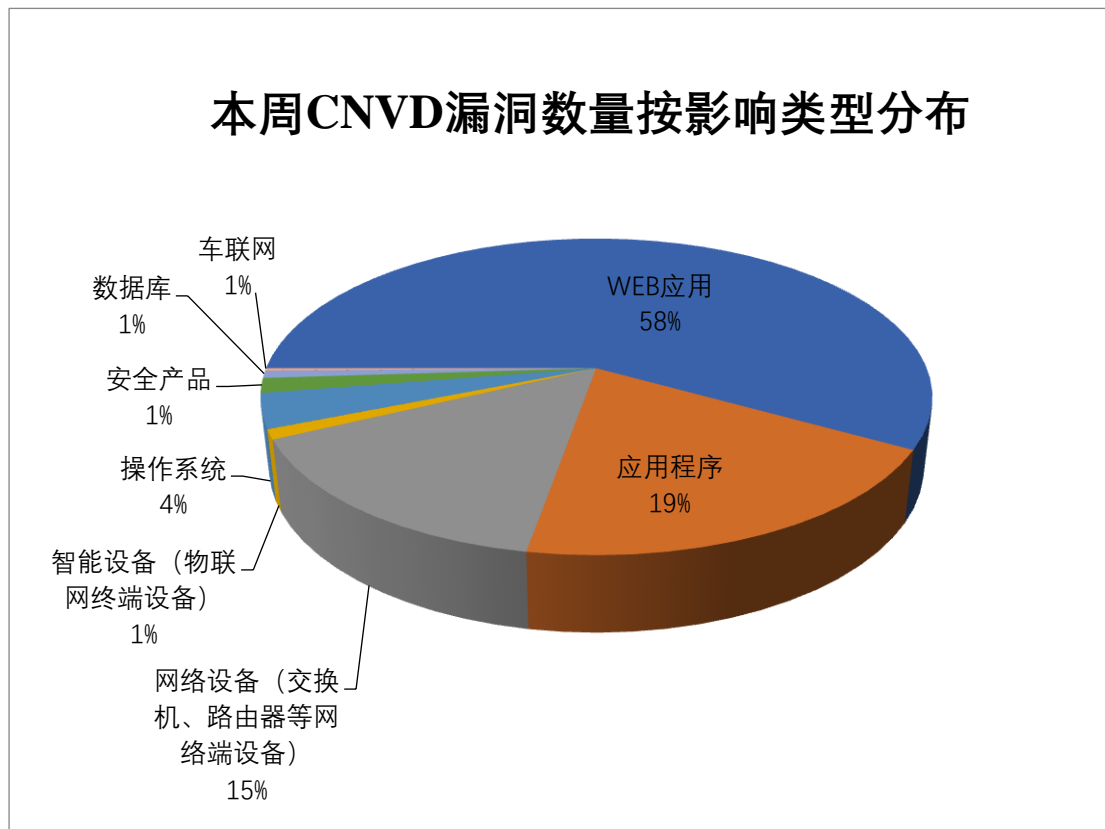


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、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	Google	14	4%
2	Adobe	12	3%
3	Siemens	12	3%
4	Mozilla	10	2%
5	北京百卓网络技术有限公司	9	2%
6	Scholars Tracking System	6	2%
7	济南驰骋信息技术有限公司	6	2%
8	点都互联科技有限公司	5	1%
9	WordPress	5	1%
10	其他	317	80%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，37 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，“Google Android 权限提升漏洞（CNVD-2023-60903）、Siemens SIMATIC CN 4100 访问控制不当漏洞”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/>

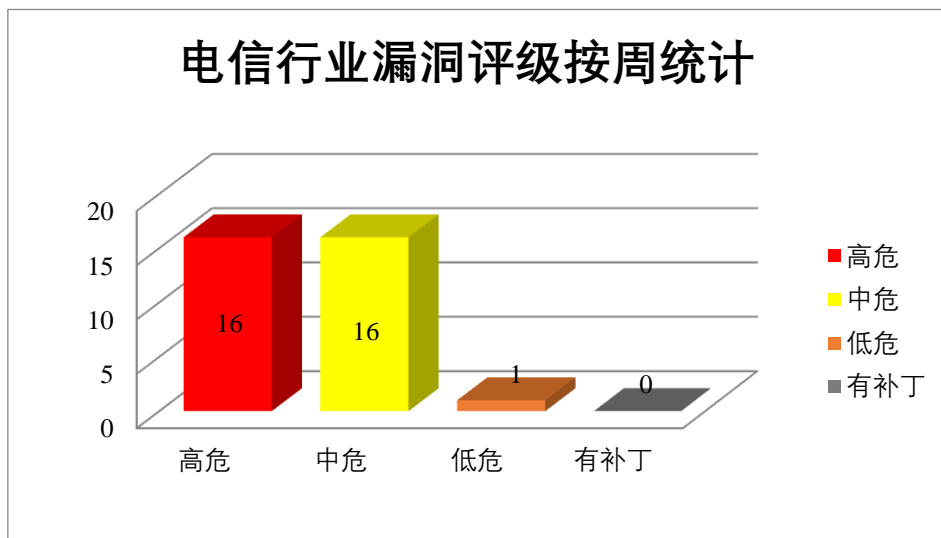


图 3 电信行业漏洞统计

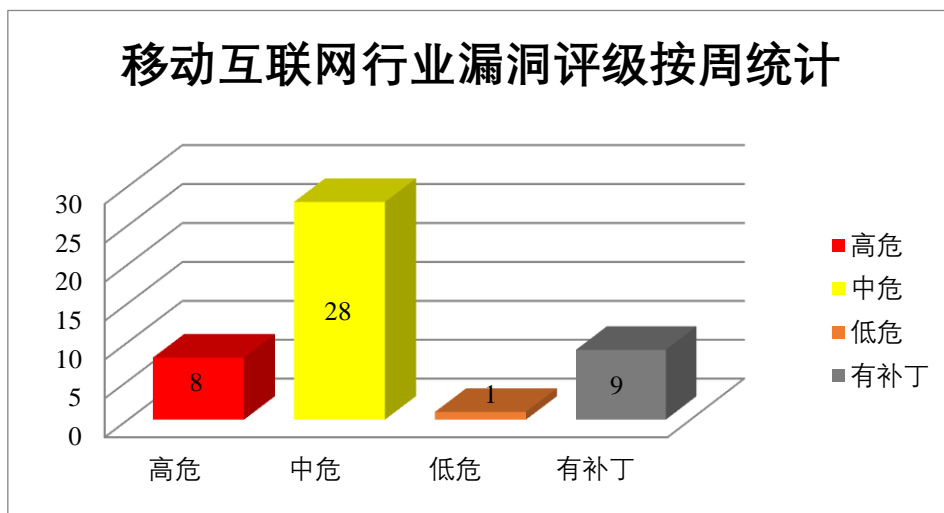


图 4 移动互联网行业漏洞统计

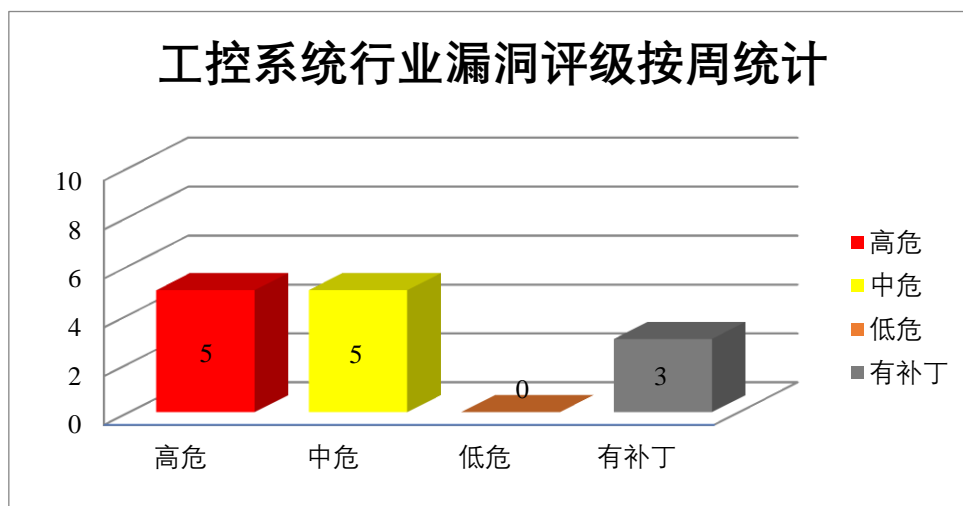


图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。本周，上述产品被披露存在越界读取漏洞，攻击者可利用漏洞导致内存泄露。

CNVD 收录的相关漏洞包括：Adobe InDesign 越界读取漏洞（CNVD-2023-59724、CNVD-2023-59723、CNVD-2023-59725、CNVD-2023-59726、CNVD-2023-59728、CNVD-2023-59727、CNVD-2023-59729、CNVD-2023-59731）。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-2023-59724>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59723>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59725>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59726>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59728>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59727>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59729>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59731>

2、Siemens 产品安全漏洞

Siemens SIMATIC CN 4100 是德国西门子（Siemens）公司的一个通信节点。RUGGEDCOM 产品提供了一定程度的稳健性和可靠性，为部署在恶劣环境中的通信网络设定了标准。Siemens Teamcenter Visualization 是德国西门子（Siemens）公司的一个可为设计 2D、3D 场景提供团队协作功能的软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码，获得管理员访问权限，从而完全控制设备等。

CNVD 收录的相关漏洞包括：Siemens SIMATIC CN 4100 访问控制不当漏洞、Siemens RUGGEDCOM ROX 命令注入漏洞（CNVD-2023-60606、CNVD-2023-60607、CNVD-2023-60609、CNVD-2023-60608、CNVD-2023-60610、CNVD-2023-60611）、Siemens Teamcenter Visualization 缓冲区溢出漏洞。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-2023-60605>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60606>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60607>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60609>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60608>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60610>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60611>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60613>

3、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。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，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2023-59950、CNVD-2023-59952、CNVD-2023-59957、CNVD-2023-59956）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-59954）、Mozilla Firefox 跨站脚本漏洞（CNVD-2023-59953）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2023-59955）、Mozilla Firefox

资源管理错误漏洞（CNVD-2023-59959）。其中，除“Mozilla Firefox 信息泄露漏洞（CNVD-2023-59950、CNVD-2023-59957）、Mozilla Firefox 跨站脚本漏洞（CNVD-2023-59953）”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-2023-59950>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59954>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59953>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59952>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59957>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59956>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59955>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-59959>

4、Google 产品安全漏洞

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。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，攻击者可利用漏洞获得提升的权限，在系统上执行任意代码或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-60890、CNVD-2023-60902、CNVD-2023-60903）、Google Android Framework 代码执行漏洞（CNVD-2023-60900、CNVD-2023-60937）、Google Android 权限提升漏洞（CNVD-2023-60938）、Google Chrome V8 代码执行漏洞（CNVD-2023-60939）、Google Chrome WebXR 代码执行漏洞。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-2023-60890>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60900>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60902>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60903>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60937>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60938>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60939>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-60940>

5、TeleAdapt RoomCast TA-2400 权限提升漏洞

TeleAdapt RoomCast TA-2400 是英国 TeleAdapt 公司的一款适用于客房的一体化、自带的顶级内容流媒体盒。本周，TeleAdapt RoomCast TA-2400 被披露存在权限提升漏

洞。该漏洞是由于 Android 调试桥（ADB）的权限管理不当造成的。攻击者可利用该漏洞获得提升的 root 权限。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-2023-61013>

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：<https://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-2023-59958	Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2023-59958）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/
CNVD-2023-60469	Froxlор 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/froxlор/froxlор/commit/03b5a921ff308eeab21bf9d240f27783c8591965
CNVD-2023-60604	Siemens SIMATIC CN 4100 默认权限不正确漏洞	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-313488.html
CNVD-2023-60612	Siemens RUGGEDCOM ROX 加密问题漏洞	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-146325.html
CNVD-2023-60621	Siemens JT Open 和 JT Utilities 越界读取漏洞	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/pdf/ssa-642810.pdf
CNVD-2023-60888	Smartbi setEngineAddress 权限绕过漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新： https://www.smartbi.com.cn/patchinfo
CNVD-2023-60941	Google Chrome WebRTC 代码执行漏洞（CNVD-2023-60941）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop_13.html
CNVD-2023-60942	Google Chrome Autofill payments 代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop_13.html

			m/2023/06/stable-channel-update-for-desktop_13.html
CNVD-2023-61173	GIT 存在服务参数注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/git/git/security/advisories/GHSA-v48j-4xgg-4844
CNVD-2023-61350	帆软 FineBI 大数据分析工具存在命令执行漏洞	高	厂商已提供漏洞修补方案，请联系厂商更新版本： https://service.fanruan.com/support

小结：本周，Adobe 产品被披露存在越界读取漏洞，攻击者可利用漏洞导致内存泄露。此外，Siemens、Mozilla、Google 等多款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，在当前进程的上下文中执行代码，获得管理员访问权限，从而完全控制设备等。另外，TeleAdapt RoomCast TA-2400 被披露存在权限提升漏洞。攻击者可利用该漏洞获得提升的 root 权限。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、Milesight UR32L firewall_handler_set 函数缓冲区溢出漏洞（CNVD-2023-61192）

验证描述

Milesight UR32L 是中国星纵物联（Milesight）公司的一个 4G 工业路由器。

Milesight UR32L firewall_handler_set 函数存在缓冲区溢出漏洞，攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致应用程序崩溃。

验证信息

POC 链接：https://talosintelligence.com/vulnerability_reports/TALOS-2023-1716

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2023-61192>

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. PaperCut 打印机管理程序漏洞遭在野攻击

PaperCut MF 与 PaperCut NG 中发现了远程执行代码漏洞，影响 22.0.9 以及更早版

本。该漏洞被确定为 CVE-2023-27350，CVSS 评分为 9.8。

参考链接：<https://www.freebuf.com/articles/network/373707.html>

2. 亚马逊云（AWS）曝新漏洞，SSM 代理已成木马！

网络安全研究人员在亚马逊云平台（AWS）中发现了一种新的后渗透攻击，能允许 AWS 系统管理器代理(SSM 代理)作为远程访问木马在 Windows 和 Linux 环境中运行。

参考链接：<https://thehackernews.com/2023/08/researchers-uncover-aws-ssm-agent.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