国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 05 月 08 日-2023 年 05 月 14 日 **2023 年第 19 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 418 个，其中高危漏洞 195 个、中危漏洞 180 个、低危漏洞 43 个。漏洞平均分值为 6.45。本周收录的漏洞中，涉及 0day 漏洞 332 个（占 79%），其中互联网上出现“Markdownify 代码执行漏洞、Perfex Crm 跨站脚本漏洞（CNVD-2023-36117）”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 4646 个，与上周（12062 个）环比减少 61%。

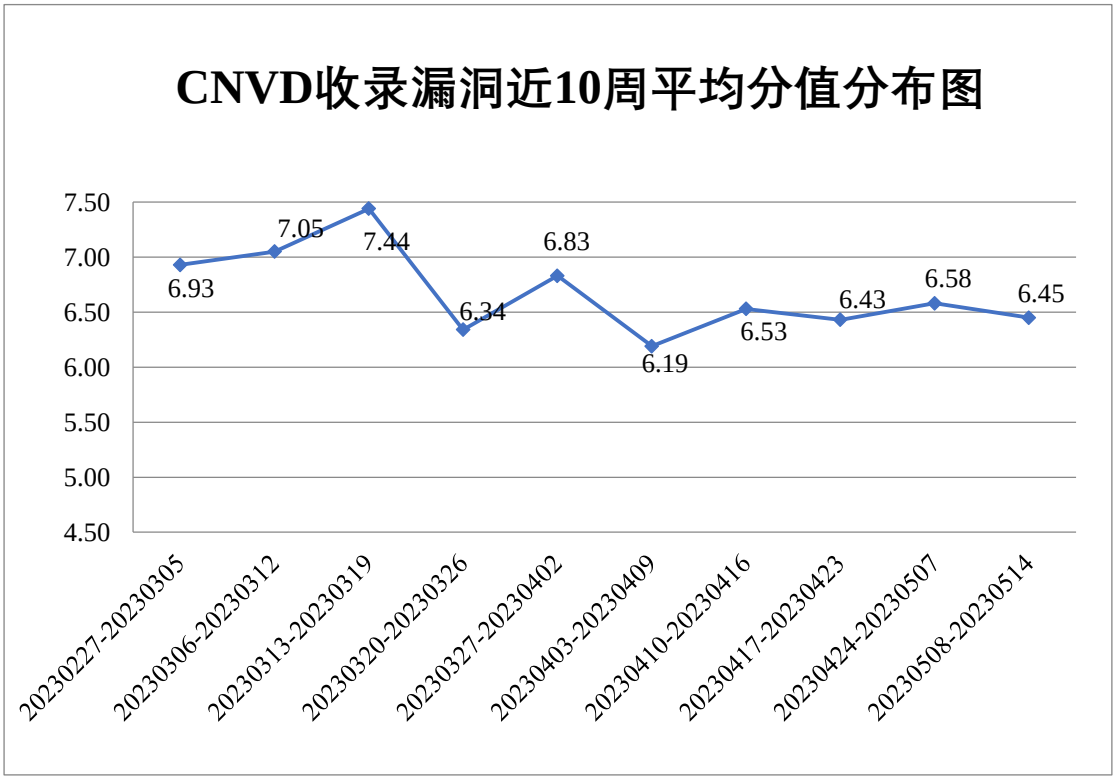

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 32 起，向基础电信企业通报漏洞事件 42 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 890 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 262 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 93 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：

紫光软件系统有限公司、珠海世纪鼎利科技股份有限公司、珠海玖时光科技有限公司、重庆金算盘软件有限公司、重庆建工信息技术有限公司、中科方德软件有限公司、织金农创电子商务有限公司、浙江甄优智能科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江核新同花顺网络信息股份有限公司、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、永辉彩食鲜发展有限公司、新开普电子股份有限公司、小船出海教育科技（北京）有限公司、西安卓立科技实业有限公司、西安瑞友信息技术资讯有限公司、武汉易维科技股份有限公司、望海康信（北京）科技股份公司、天维尔信息科技股份有限公司、天津天堰科技股份有限公司、天津神州浩天科技有限公司、天津点滴记忆信息科技有限公司、腾讯安全应急响应中心、拓尔思信息技术股份有限公司、四川众联臻致信息技术有限公司、四川迅睿云软件开发有限公司、施耐德电气（中国）有限公司、神州数码控股有限公司、深圳市云联友科科技有限公司、深圳市深科特信息技术有限公司、深圳市磊科实业有限公司、深圳市捷道智控实业有限公司、深圳市甲天行科技有限公司、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、深圳市博思高科技有限公司、上海卓卓网络科技有限公司、上海商派网络科技有限公司、上海桑锐电子科技股份有限公司、上海人宝实业集团有限公司、上海擎创信息技术有限公司、上海吉的堡教育软件开发有限公司、上海泛微网络科技股份有限公司、上海冰峰计算机网络技术有限公司、熵基科技股份有限公司、商丘芝麻开门网络科技有限公司、山西大昌电子商务有限公司、山石网科通信技术股份有限公司、厦门泰博科技有限公司、厦门四信通信科技有限公司、厦门狄耐克智能科技股份有限公司、软通农科信息技术（武汉）有限公司、泉州扬荣信息科技有限公司、青岛东软载波科技股份有限公司、普联技术有限公司、内蒙古优然牧业有限责任公司、南宁迈世信息技术有限公司、南京先极科技有限公司、南京汇微达信息技术有限公司、联奕科技股份有限公司、焦点教育科技有限公司、江西金磊科技发展有限公司、江苏中威科技软件系统有限公司、江苏万林现代物流股份有限公司、江苏省广电有线信息网络股份有限公司、江苏兰德数码科技有限公司、江苏达实久信医疗科技有限公司、江苏安科瑞电器制造有限公司、济南驰骋信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南省众达数蔚信息技术有限公司、湖南翱云网络科技有限公司、

弘扬软件股份有限公司、杭州叙简科技股份有限公司、杭州施强教育科技有限公司、杭州绿洁科技股份有限公司、杭州海康威视数字技术股份有限公司、杭州达罗尼科技有限公司、哈尔滨新中新电子股份有限公司、国信云联数据科技股份有限公司、广州自我游网络科技有限公司、广州中望龙腾软件股份有限公司、广州红帆科技有限公司、广西师范大学出版社集团有限公司、广东凯格科技有限公司、广东博宏药业有限公司、福州网钛软件科技有限公司、福州联迅信息科技有限公司、东方电子股份有限公司、东北师大理想软件股份有限公司、成都青软青之软件有限公司、成都普什信息自动化有限公司、成都光大网络科技有限公司、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、北京易华录信息技术股份有限公司、北京阳光百校教育科技有限公司、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、北京通达信科科技有限公司、北京胜能能源科技有限公司、北京人大金仓信息技术股份有限公司、北京摩梭科技有限公司、北京龙软科技股份有限公司、北京朗新天霁软件技术有限公司、北京坤豆科技有限公司、北京卡车之家信息技术股份有限公司、北京经观文化传媒有限公司、北京飞书科技有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、安吉畅游汽车服务股份有限公司、阿里巴巴集团安全应急响应中心、zzzcms、TrueCMS、SEMCMS和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周，CNVD 发布了《Microsoft 发布 2023 年 5 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8831

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、北京神州绿盟科技有限公司、安天科技集团股份有限公司、深信服科技股份有限公司、北京数字观星科技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、重庆电信系统集成公司、上海齐同信息科技有限公司、联想集团、安徽锋刃信息科技有限公司、北京升鑫网络科技有限公司、内蒙古洞明科技有限公司、河南信安世纪科技有限公司、河南东方云盾信息技术有限公司、山东正中信息技术股份有限公司、中孚安全技术有限公司、杭州默安科技有限公司、湖南轻山信息技术有限公司、杭州海康威视数字技术股份有限公司、浙江中控技术股份有限公司、赛尔网络有限公司、山东云天安全技术有限公司、河北锝远网络科技有限公司、南京深安科技有限公司、北京山石网科信息技术有限公司、国网智能电网研究院有限公司、上海嘉韦思信息技术有限公司、任子行网络技术股份有限公司、深圳市智安网络有限公司、北京安帝科技有限公司、北京六方云信息技术有限公司、广州安亿信软件科技有限公司、北京君云天下科技有限公司、辽宁省烟草公司营口市公司、重庆易阅科技有限公司、建信金科网络攻击实验室、河南悦海数安科技有限公司、

上海谋乐网络科技有限公司、福建省海峡信息技术有限公司、华堡天建（天津）信息技术有限公司、超聚变数字技术有限公司、宁夏凯信特信息科技有限公司、郑州埃文科技、博智安全科技股份有限公司及其他个人白帽子向 CNVD 提交了 4646 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）和上海交大向 CNVD 共享的白帽子报送的 1852 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
斗象科技（漏洞盒子）	1157	1157
新华三技术有限公司	706	0
北京神州绿盟科技有限公司	496	2
奇安信网神（补天平台）	432	432
安天科技集团股份有限公司	377	2
深信服科技股份有限公司	360	0
上海交大	263	263
北京数字观星科技有限公司	149	0
阿里云计算有限公司	111	3
北京天融信网络安全技术有限公司	104	3
北京启明星辰信息安全技术有限公司	98	24
远江盛邦（北京）网络安全科技股份有限公司	80	80
京东科技信息技术有限公司	34	7
天津市国瑞数码安全系统股份有限公司	34	0
中国电信集团系统集成有限责任公司	27	1
杭州安恒信息技术股	22	22

份有限公司		
杭州迪普科技股份有限公司	15	0
北京智游网安科技有限公司	3	3
北京长亭科技有限公司	3	3
浙江大华技术股份有限公司	3	3
南京铱迅信息技术股份有限公司	1	1
华为技术有限公司	1	1
西安四叶草信息技术有限公司	1	1
北京知道创宇信息技术股份有限公司	1	0
快页信息技术有限公司	415	415
重庆电信系统集成公司	97	97
上海齐同信息科技有限公司	80	80
联想集团	40	40
安徽锋刃信息科技有限公司	29	29
北京升鑫网络科技有限公司	27	27
西门子（中国）有限公司	22	0
内蒙古洞明科技有限公司	22	22
河南信安世纪科技有限公司	17	17
河南东方云盾信息技术有限公司	14	14

山东正中信息技术股份有限公司	10	10
中孚安全技术有限公司	8	8
杭州默安科技有限公司	8	8
湖南轻山信息技术有限公司	7	7
杭州海康威视数字技术股份有限公司	6	6
浙江中控技术股份有限公司	6	6
赛尔网络有限公司	5	5
山东云天安全技术有限公司	5	5
河北镌远网络科技有限公司	4	4
南京深安科技有限公司	3	3
北京山石网科信息技术有限公司	3	3
国网智能电网研究院有限公司	3	3
上海嘉韦思信息技术有限公司	3	3
任子行网络技术股份有限公司	2	2
深圳市智安网络有限公司	2	2
北京安帝科技有限公司	2	2
北京六方云信息技术有限公司	2	2
广州安亿信软件科技有限公司	2	2

北京君云天下科技有限公司	1	1
辽宁省烟草公司营口市公司	1	1
重庆易阅科技有限公司	1	1
建信金科网络攻击实验室	1	1
河南悦海数安科技有限公司	1	1
上海谋乐网络科技有限公司	1	1
福建省海峡信息技术有限公司	1	1
华堡天建（天津）信息技术有限公司	1	1
超聚变数字技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
郑州埃文科技	1	1
博智安全科技股份有限公司	1	1
CNCERT 广西分中心	2	2
CNCERT 北京分中心	1	1
个人	1801	1801
报送总计	7138	4646

本周漏洞按类型和厂商统计

本周，CNVD 收录了 418 个漏洞。WEB 应用 231 个，应用程序 76 个，网络设备（交换机、路由器等网络端设备）74 个，操作系统 28 个，智能设备（物联网终端设备）7 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	231
应用程序	76
网络设备（交换机、路由器等网络端设备）	74
操作系统	28
智能设备（物联网终端设备）	7
安全产品	2

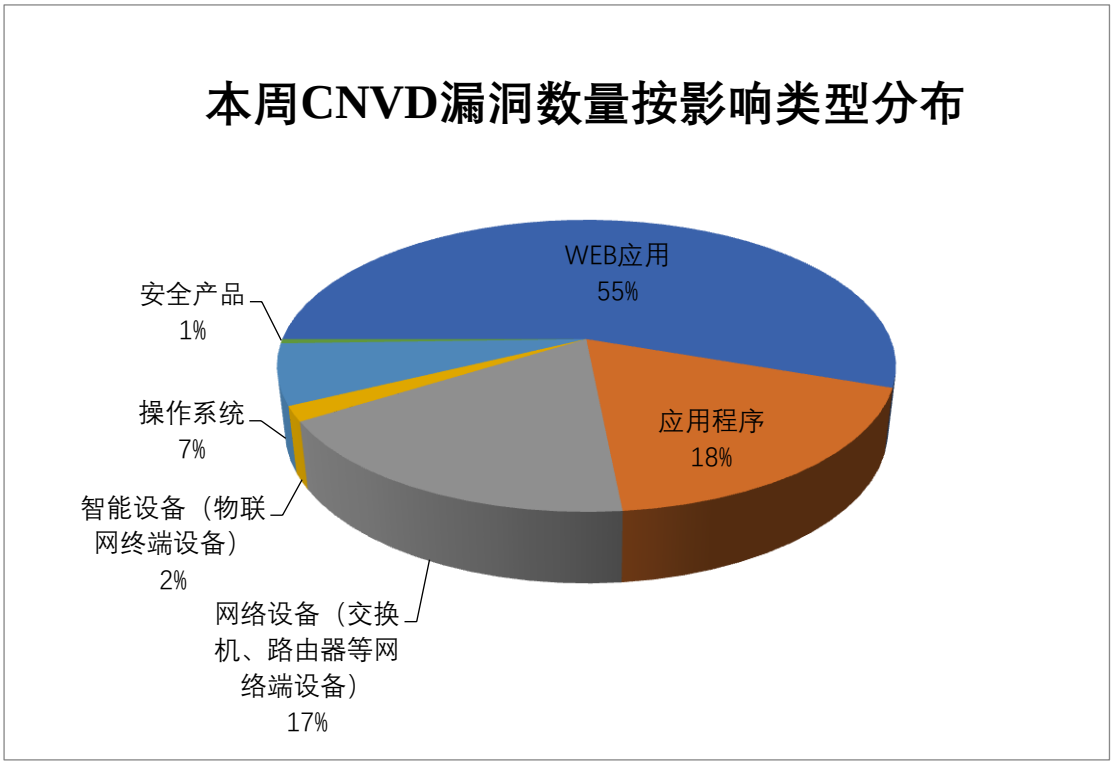

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Microsoft、Linux 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	21	5%
2	Microsoft	15	4%
3	Linux	15	4%
4	Google	13	3%
5	TOTOLINK	10	3%
6	北京百卓网络技术有限公司	9	2%
7	北京网康科技有限公司	6	1%
8	厦门市灵鹿谷科技有限公司	5	1%
9	WordPress	5	1%

10	其他	319	76%

本周行业漏洞收录情况

本周，CNVD 收录了 35 个电信行业漏洞，49 个移动互联网行业漏洞，29 个工控行业漏洞（如下图所示）。其中，“Zyxel NBG6604 命令注入漏洞、Google Android 权限提升漏洞（CNVD-2023-36105）、Siemens SIMATIC Cloud Connect 7 路径遍历漏洞”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/

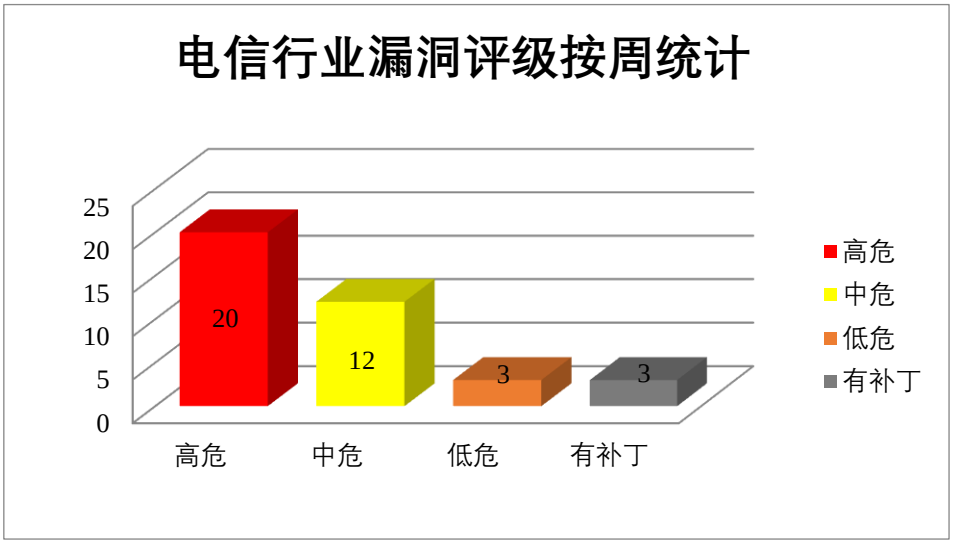

图 3 电信行业漏洞统计

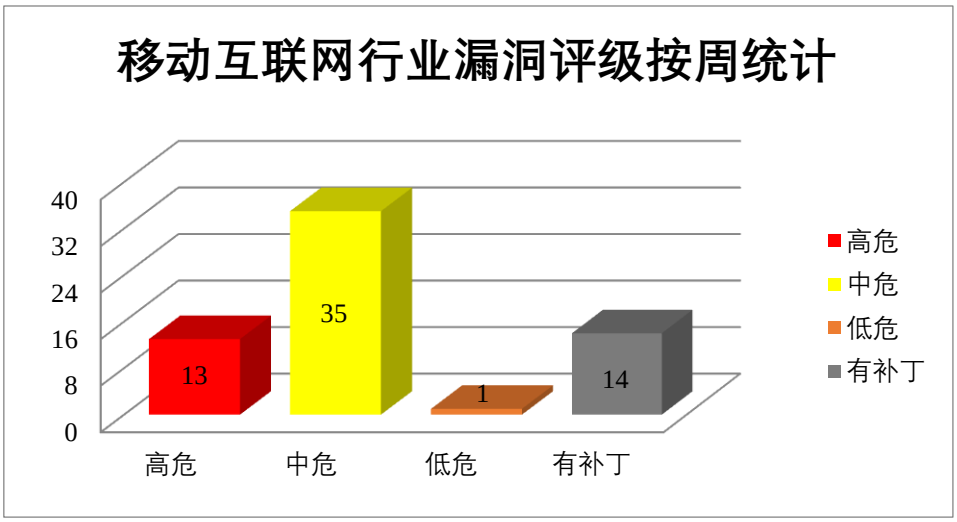

图 4 移动互联网行业漏洞统计

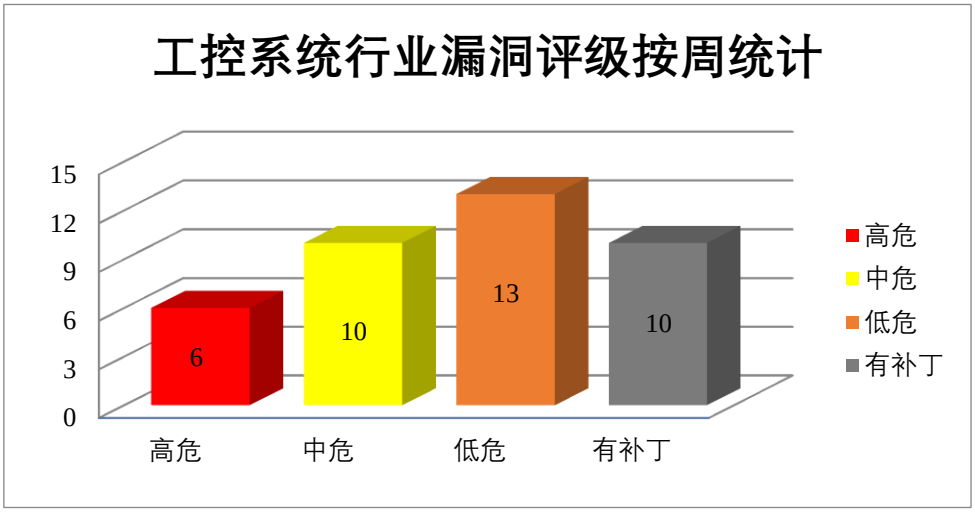

图 5 工控系统行业漏洞统计

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、 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。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，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-36105、CNVD-2023-36108、CNVD-2023-36107、CNVD-2023-36109、CNVD-2023-36112、CNVD-2023-36115、CNVD-2023-36114）、Google Android 代码执行漏洞（CNVD-2023-36113）。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-2023-36105
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36108
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36107
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36109
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36113
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36112
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36115
https://www.cnvd.org.cn/flaw/show/CNVD-2023-36114

2、 Siemens 产品安全漏洞

Siemens TIA Portal 是德国西门子（Siemens）公司的一个完全集成的自动化门户。TIA Portal 使您可以不受限制地访问从数字规划到集成工程和透明操作的全套数字化自

动化服务。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。SIMATIC Cloud Connect 7 是一种物联网网关，用于将可编程逻辑控制器连接到云服务，并允许将现场设备与 OPC UA 服务器接口连接为 OPC UA 客户端。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端点下载可用的文件，执行任意代码，导致拒绝服务（DoS）等。

CNVD 收录的相关漏洞包括：Siemens TIA Portal 路径遍历漏洞（CNVD-2023-35760）、Siemens Solid Edge 文件解析漏洞（CNVD-2023-35762）、Siemens SIMATIC Cloud Connect 7 路径遍历漏洞（CNVD-2023-35768、CNVD-2023-35772）、Siemens SIMATIC Cloud Connect 7 信息泄露漏洞（CNVD-2023-35770、CNVD-2023-35769）、Siemens SIMATIC Cloud Connect 7 拒绝服务漏洞、Siemens SIMATIC Cloud Connect 7 命令注入漏洞。其中，“Siemens Solid Edge 文件解析漏洞（CNVD-2023-35762）、Siemens SIMATIC Cloud Connect 7 路径遍历漏洞（CNVD-2023-35772）、Siemens SIMATIC Cloud Connect 7 命令注入漏洞”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-2023-35760
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35762
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35768
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35770
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35769
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35772
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35771
https://www.cnvd.org.cn/flaw/show/CNVD-2023-35774

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。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内核信息泄露，权限提升，使服务器崩溃，执行任意代码等。

CNVD 收录的相关漏洞包括：Linux kernel tcindex_delete 函数内存错误引用漏洞、Linux Kernel 拒绝服务漏洞（CNVD-2023-34458）、Linux kernel 资源管理错误漏洞（CNVD-2023-34463、CNVD-2023-34467、CNVD-2023-34465）、Linux kernel 权限提升漏洞（CNVD-2023-34461）、Linux kernel 双重释放漏洞（CNVD-2023-34466）、Linux kernel 输入验证错误漏洞（CNVD-2023-34464）。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-2023-34460

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34458

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34463

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34461

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34467

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34466

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34465

https://www.cnvd.org.cn/flaw/show/CNVD-2023-34464

4、Microsoft 产品安全漏洞

Microsoft PostScript Printer Driver 是美国微软（Microsoft）公司的用于 PostScript 打印机的 Microsoft 标准打印机驱动程序。Microsoft PCL6 Class Printer Driver 是美国微软（Microsoft）公司的一个打印机驱动软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞远程执行代码。

CNVD 收录的相关漏洞包括：Microsoft PostScript and PCL6 Class Printer Driver 远程代码执行漏洞（CNVD-2023-35215、CNVD-2023-35213、CNVD-2023-35212、CNVD-2023-35218、CNVD-2023-35217、CNVD-2023-35216、CNVD-2023-35221、CNVD-2023-35220）。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-2023-35215

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35213

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35212

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35218

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35217

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35216

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35221

https://www.cnvd.org.cn/flaw/show/CNVD-2023-35220

5、NETGEAR R6220 命令执行漏洞

NETGEAR R6220 是美国网件（NETGEAR）公司的一款无线路由器。本周，NETGEAR R6220 被披露存在命令执行漏洞，该漏洞是由于访问控制不当造成的。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-2023-36121

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-2023-35222	Microsoft PostScript and PCL6 Class Printer Driver 远程代码执行漏洞（CNVD-2023-35222）	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-2023-24887
CNVD-2023-35225	Microsoft PostScript and PCL6 Class Printer Driver 远程代码执行漏洞（CNVD-2023-35225）	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-2023-21684
CNVD-2023-35756	多款 Siemens 产品拒绝服务漏洞（CNVD-2023-35756）	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-566905.pdf
CNVD-2023-35758	多款 Siemens 产品拒绝服务漏洞（CNVD-2023-35758）	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-566905.pdf
CNVD-2023-35776	Siemens Siveillance Video 代码执行漏洞	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-789345.html
CNVD-2023-35775	Siemens Siveillance Video 代码执行漏洞（CNVD-2023-35775）	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-789345.html
CNVD-2023-36110	Google Android 越界写入漏洞（CNVD-2023-36110）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/2023-03-01
CNVD-2023-36283	AzuraCast 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/azuracast/azuracast/commit/bdb23594ad3e0c47c8568ce028a7c244a406cf9d
CNVD-2023-36292	Zyxel NBG6604 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router
CNVD-2023-36315	TOTOLINK X18 setDiagnosisCfg 函数命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系

统上执行任意代码。此外，Siemens、Linux、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过端点下载可用的文件，导致内核信息泄露，权限提升，执行任意代码，导致拒绝服务（DoS）等。另外，NETGEAR R6220 被披露存在命令执行漏洞，攻击者可利用该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、Markdownify 代码执行漏洞

验证描述

Markdownify 是一个基于 Electron 构建的最小 Markdown Editor 桌面应用程序。

Markdownify 存在代码执行漏洞。该漏洞源于外部输入数据构造代码段的过程中，网络系统或产品未能正确过滤其中的特殊元素。攻击者可利用漏洞执行任意代码。

验证信息

POC 链接：https://fluidattacks.com/advisories/adams/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-36120

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. 安全漏洞使 WordPress 网站被劫持

流行的 WordPress 插件 Essential Addons for Elementor 中披露了一个安全漏洞，该漏洞可能被利用来在受影响的站点上获得提升的权限。

参考链接：https://thehackernews.com/2023/05/severe-security-flaw-exposes-over.html

2. 8.5w+ MS Exchange 服务器仍然受到 RCE 漏洞影响

Cyber news 调查显示，自微软敦促组织更新其软件以修补 Exchange 服务器上的漏洞以来的几个月，仍有超过 8.5w 台服务器受到攻击。

参考链接：https://cybernews.com/security/ms-exchange-servers-vulnerable-rce-bugs/

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