国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 06 月 14 日-2021 年 06 月 20 日　　2021 年第 24 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 494 个，其中高危漏洞 172 个、中危漏洞 283 个、低危漏洞 39 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 298 个（占 60%），其中互联网上出现“bloofoxCMS 跨站请求伪造漏洞（CNVD-2021-43375）、OpenText Content Server 'multiple'跨站脚本漏洞”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事件型漏洞总数 2579 个，与上周（3991 个）环比减少 35%。

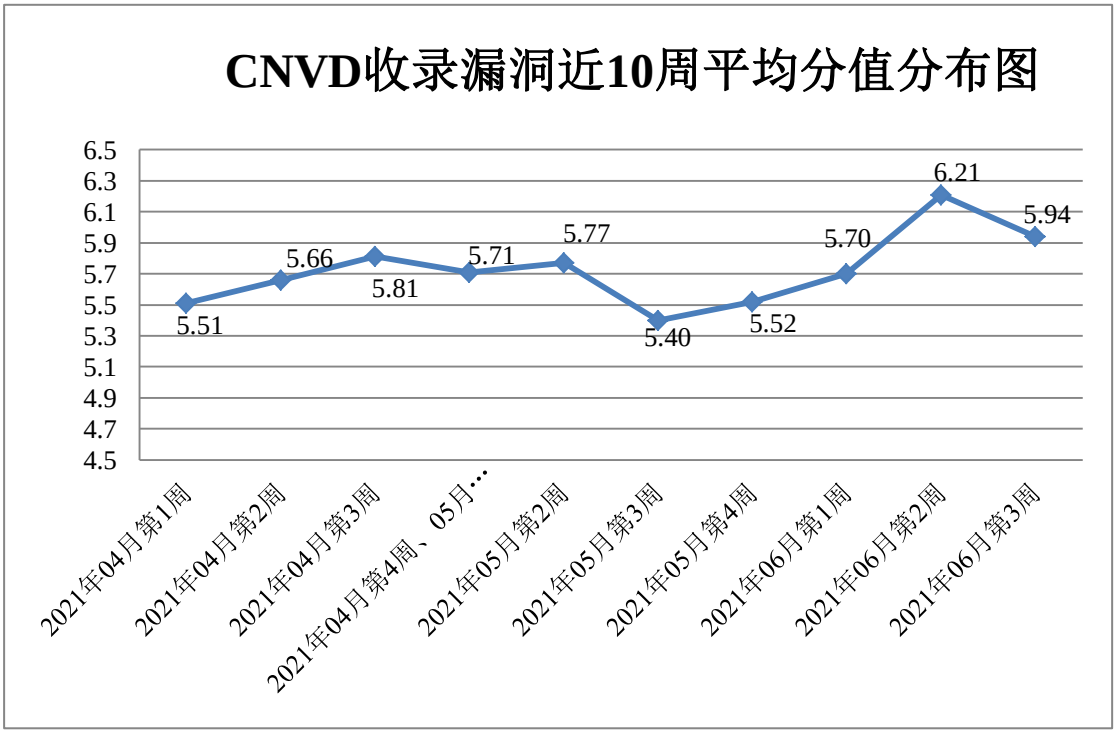

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电信企业通报漏洞事件 11 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 228 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 36 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 33 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：

珠海市魅族科技有限公司、重庆远秋科技有限公司、中山市华拓信息技术有限公司、中科宁图技术江苏有限公司、中国大唐集团有限公司、郑州天迈科技股份有限公司、浙江图讯科技股份有限公司、浙江禾匠信息科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、西安众邦网络科技有限公司、武汉市公共交通集团有限责任公司、武汉类森科技有限公司、武汉东信同邦信息技术有限公司、武汉初心科技有限公司、潍坊家园驿站电子技术有限公司、微软（中国）有限公司、网宿科技股份有限公司、天地伟业技术有限公司、苏州科达科技股份有限公司、四川五佳网络科技有限公司、四川时来科技有限公司、思科系统（中国）网络技术有限公司、施耐德电气（中国）有限公司、神州数码集团股份有限公司、深圳宜搜天下科技股份有限公司、深圳市子辰视讯科技有限公司、深圳市中科网威科技有限公司、深圳市中电电力技术股份有限公司、深圳市微耕实业有限公司、深圳市网域科技技术有限公司、深圳市腾讯计算机系统有限公司、深圳市联天通信技术有限公司、深圳市朗驰欣创科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市和为顺网络技术有限公司、深信服科技股份有限公司、上海新朋程数据科技发展有限公司、上海梦之路数字科技有限公司、上海旅烨网络科技有限公司、上海力软信息技术有限公司、上海肯特仪表股份有限公司、上海华依科技有限公司、上海互盾信息科技有限公司、上海斐讯数据通信技术有限公司、上海丹帆网络科技有限公司、上海博达数据通信有限公司、山石网科通信技术（北京）有限公司、山东鼎软天下信息技术有限公司、厦门狮子鱼网络科技有限公司、厦门得推网络科技有限公司、睿峰网云（北京）科技股份有限公司、瑞斯康达科技发展股份有限公司、锐捷网络股份有限公司、任子行网络技术股份有限公司、南通万嘉网络科技有限公司、南宁得实科技有限公司、迈普通信技术股份有限公司、江苏中威科技信息系统有限公司、江苏易索电子科技股份有限公司、济南爱程网络科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、黑龙江立高科技股份有限公司、杭州品茗信息技术有限公司、杭州会搜科技股份有限公司、杭州海康威视数字技术股份有限公司、杭州艾朴软件有限公司、广州协众软件科技有限公司、广州图创计算机软件开发有限公司、广州市凝智科技有限公司、广州达讯云商网络科技有限公司、广西桂天能源集团有限公司、广东星神科技有限公司、福建星网智慧科技有限公司、烽

火通信科技股份有限公司、鼎点视讯科技有限公司、大唐电信科技股份有限公司、成都智蜂网科技有限责任公司、成都星锐蓝海网络科技有限公司、成都强时科技有限公司、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、北京智敏科技发展有限公司、北京云中融信网络科技有限公司、北京亿赛通科技发展有限责任公司、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、北京网御星云信息技术有限公司、北京同方信息安全技术股份有限公司、北京圣博润高新技术股份有限公司、北京酷我科技有限公司、北京康海时代科技有限公司、北京华夏大地远程教育网络服务有限公司、北京和欣运达科技有限公司、北京翰博尔信息技术股份有限公司、北京多点在线科技有限公司、北京大麦地信息技术有限公司、北京百卓网络技术有限公司、百度安全应急响应中心、阿里巴巴集团安全应急响应中心、商合行、贴心猫（imcat）、千旺软件、vivo 安全团队、OPPO 安全应急响应中心、Buffalo 公司、YXCMS、Yawcam、Trendnet、The Apache Software Foundation、Teledyne FLIR、SEH Computertechnik GmbH、RPCMS、Power Software Ltd、Maccms、Kpcms、foru cms、Bluecms 和 Axis Communications AB。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京数字观星科技有限公司、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。广州易东信息安全技术有限公司、河南灵创电子科技有限公司 、南京众智维信息科技有限公司、北京山石网科信息技术有限公司、江西省掌控者信息安全技术有限公司、河南信安世纪科技有限公司、北京信联科汇科技有限公司、北京禹宏信安科技有限公司、北京华云安信息技术有限公司、重庆都会信息科技有限公司、北京天地和兴科技有限公司、杭州木链物联网科技有限公司、杭州迪普科技股份有限公司、杭州天谷信息科技有限公司、武汉明嘉信信息安全检测评估有限公司、北京安帝科技有限公司、星云博创科技有限公司、山东云天安全技术有限公司、江苏晟晖信息科技有限公司、联想全球安全实验室、安徽长泰信息安全服务有限公司、平安银河实验室、山东泽鹿安全技术有限公司、长春嘉诚信息技术股份有限公司、北京机沃科技有限公司、北京远禾科技有限公司、博智安全科技股份有限公司、广州安亿信软件科技有限公司、江苏智慧安全可信技术研究院、南京树安信息技术有限公司、三门峡崤云安全服务有限公司、北京蓝森科技有限公司、亚信科技（成都）有限公司、浙江御安信息技术有限公司、中移（杭州）信息技术有限公司、河北千诚电子科技有限公司及其他个人白帽子向 CNVD 提交了 2579 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 1097 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）	570	570
上海交大	337	337
哈尔滨安天科技集团股份有限公司	217	0
奇安信网神（补天平台）	190	190
北京数字观星科技有限公司	148	0
北京神州绿盟科技有限公司	146	11
北京启明星辰信息安全技术有限公司	129	0
恒安嘉新（北京）科技股份公司	120	0
国瑞数码零点实验室	118	0
北京天融信网络安全技术有限公司	101	1
深信服科技股份有限公司	54	2
华为技术有限公司	53	0
卫士通信息产业股份有限公司	25	0
新华三技术有限公司	19	0
北京奇虎科技有限公司	6	6
北京知道创宇信息技术股份有限公司	3	0
内蒙古奥创科技有限公司	2	2
广州易东信息安全技术有限公司	384	384
河南灵创电子科技有限公司	168	168

南京众智维信息科技有限公司	117	117
北京山石网科信息技术有限公司	56	56
江西省掌控者信息安全技术有限公司	33	33
河南信安世纪科技有限公司	31	31
北京信联科汇科技有限公司	22	22
北京禹宏信安科技有限公司	20	20
中国电信股份有限公司网络安全产品运营中心	20	0
北京华云安信息技术有限公司	19	19
重庆都会信息科技有限公司	17	17
北京天地和兴科技有限公司	15	15
杭州木链物联网科技有限公司	13	13
杭州迪普科技股份有限公司	12	0
杭州天谷信息科技有限公司	7	7
武汉明嘉信信息安全检测评估有限公司	7	7
北京安帝科技有限公司	6	6
星云博创科技有限公司	6	6
山东云天安全技术有限公司	5	5

江苏晟晖信息科技有限公司	4	4
联想全球安全实验室	3	3
安徽长泰信息安全服务有限公司	2	2
平安银河实验室	2	2
山东泽鹿安全技术有限公司	2	2
长春嘉诚信息技术股份有限公司	2	2
北京机沃科技有限公司	1	1
北京远禾科技有限公司	1	1
博智安全科技股份有限公司	1	1
广州安亿信软件科技有限公司	1	1
江苏智慧安全可信技术研究院	1	1
南京树安信息技术有限公司	1	1
三门峡崤云安全服务有限公司	1	1
北京蓝森科技有限公司	1	1
亚信科技（成都）有限公司	1	1
浙江御安信息技术有限公司	1	1
中移（杭州）信息技术有限公司	1	1
河北千诚电子科技有限公司	1	1

CNCERT 宁夏分中心	10	10
CNCERT 青海分中心	2	2
CNCERT 山西分中心	2	2
个人	493	493
报送总计	3730	2579

本周漏洞按类型和厂商统计

本周，CNVD 收录了 494 个漏洞。WEB 应用 186 个，应用程序 159 个，操作系统 61 个，网络设备（交换机、路由器等网络端设备）59 个，安全产品 18 个，智能设备（物联网终端设备）9 个，数据库 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	186
应用程序	159
操作系统	61
网络设备（交换机、路由器等网络端设备）	59
安全产品	18
智能设备（物联网终端设备）	9
数据库	2

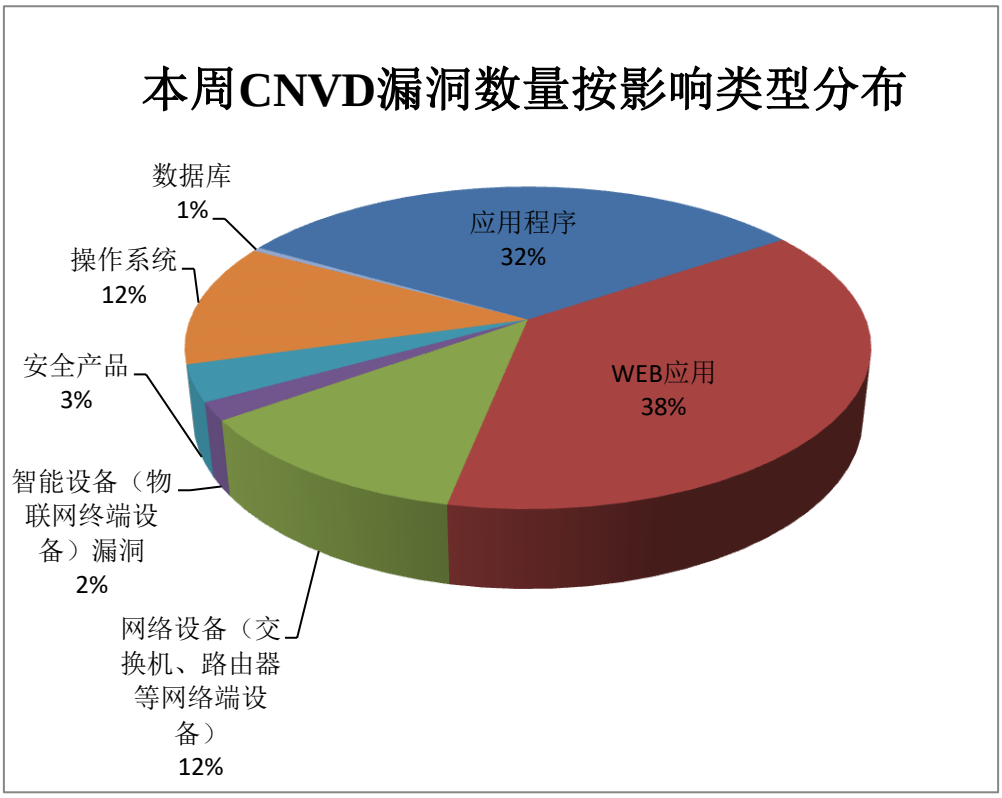

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 OpenText、Google、南宁旭东网络科技有限公司等多家厂商的产品，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	OpenText	35	7%
2	Google	34	7%
3	南宁旭东网络科技有限公司	32	7%
4	Cisco	22	4%
5	JerryScript	20	4%
6	SAP	20	4%
7	Linux	14	3%
8	Schneider Electric	14	3%
9	FFmpeg	10	2%
10	其他	293	59%

本周行业漏洞收录情况

本周，CNVD 收录了 36 个电信行业漏洞，38 个移动互联网行业漏洞，24 个工控行业漏洞（如下图所示）。其中，“Cisco IOS 和 IOS XE 拒绝服务漏洞（CNVD-2021-43438）、Google Android 权限提升漏洞（CNVD-2021-43381）、Google Android System 远程代码执行漏洞（CNVD-2021-43417）”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/

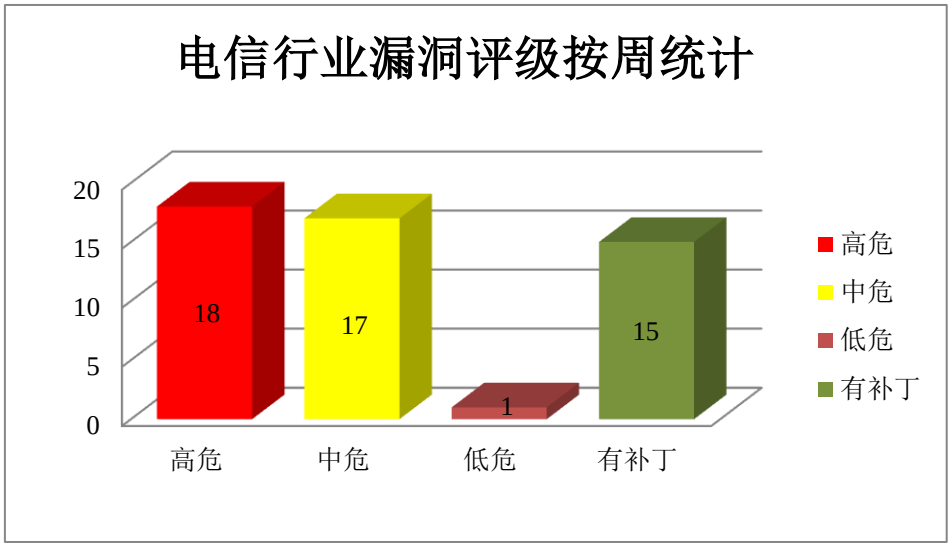

图 3 电信行业漏洞统计

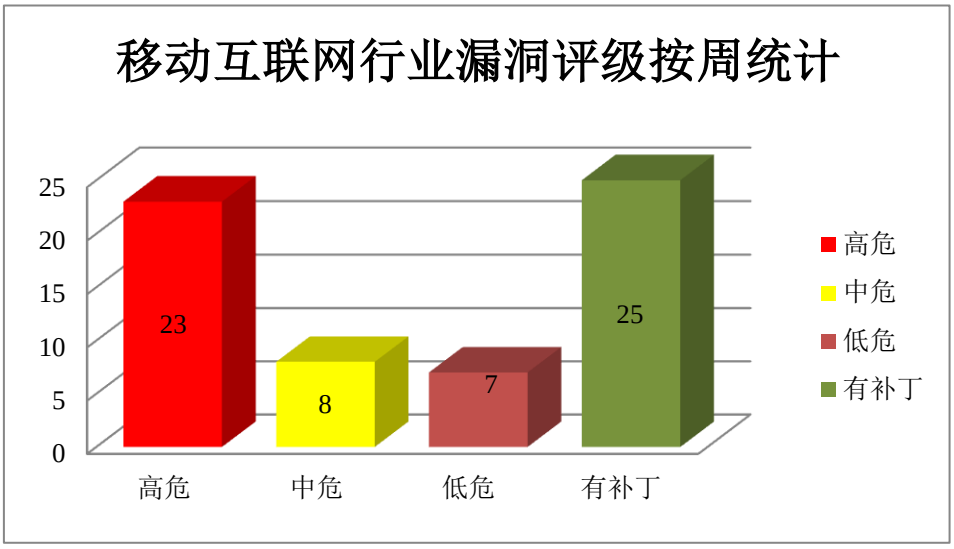

图 4 移动互联网行业漏洞统计

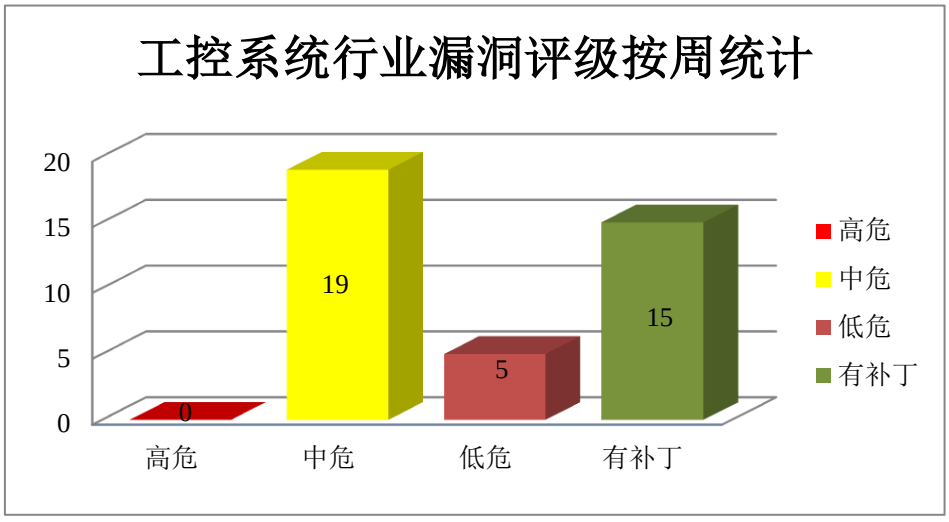

图 5 工控系统行业漏洞统计

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、 Schneider Electric 产品安全漏洞

Schneider Electric Interactive Graphical SCADA System (IGSS)是用于监测和控制工业过程的先进的 SCADA 系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取数据或实现远程代码执行。

CNVD 收录的相关漏洞包括：Interactive Graphical SCADA System (IGSS)越界写入漏洞（CNVD-2021-42155、CNVD-2021-42154、CNVD-2021-42158、CNVD-2021-42157、CNVD-2021-42159）、Interactive Graphical SCADA System (IGSS)越界读取漏洞（CNVD-2021-42153、CNVD-2021-42152、CNVD-2021-42156）。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-2021-42155

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42154

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42153

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42152

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42158

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42157

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42156

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42159

2、SAP 产品安全漏洞

SAP Netweaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台。该平台主要为 SAP 应用程序提供开发和运行环境。SAP 3D Visual Enterprise Viewer 是一款适用于 Windows 的免费 3D 可视化查看器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问受限信息，通过恶意 GIF 文件利用该漏洞导致应用程序崩溃。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS JAVA 信息泄露漏洞（CNVD-2021-42411）、SAP 3D Visual Enterprise Viewer 输入验证错误漏洞（CNVD-2021-42416、CNVD-2021-42415、CNVD-2021-42414、CNVD-2021-42419、CNVD-2021-42418、CNVD-2021-42417、CNVD-2021-42421）。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-2021-42411

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42416

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42415

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42414

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42419

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42418

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42417

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42421

3、OpenText 产品安全漏洞

OpenText Brava! Desktop 是一款基于 Windows 的查看和协作工具，可让您轻松查看几乎任何文件并进行协作。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。

CNVD 收录的相关漏洞包括：OpenText Brava! Desktop 堆缓冲区溢出漏洞（CNVD-2021-42315、CNVD-2021-42321、CNVD-2021-42319）、OpenText Brava! Desktop 越界写入漏洞（CNVD-2021-42318、CNVD-2021-42322、CNVD-2021-42320）、OpenText

Brava! Desktop 类型混淆漏洞、OpenText Brava! Desktop 远程代码执行漏洞。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-2021-42315

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42318

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42317

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42316

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42322

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42321

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42320

https://www.cnvd.org.cn/flaw/show/CNVD-2021-42319

4、Linux 产品安全漏洞

Linux kernel 是一种计算机操作系统内核，以 C 语言和汇编语言写成，符合 POSIX 标准，按 GNU 通用公共许可证发行。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 Linux 内核的 perf_mmap_close（）触发内存损坏，以触发拒绝服务并可能运行代码，生成非法的代码段，修改网络系统或组件的预期的执行控制流。

CNVD 收录的相关漏洞包括：Linux kernel 释放后重用漏洞（CNVD-2021-43363、CNVD-2021-43364）、Linux kernel llcp_sock_connect()内存泄露漏洞、Linux kernel perf_mmap_close 内存损坏漏洞、Linux kernel llcp_sock_bind()拒绝服务漏洞、Linux kernel llcp_sock_connect()权限提升漏洞、Linux kernel Zero Length Bvec 代码问题漏洞、Linux kernel 代码注入漏洞（CNVD-2021-43385）。其中，“Linux kernel llcp_sock_bind()拒绝服务漏洞、Linux kernel 释放后重用漏洞（CNVD-2021-43364）、Linux kernel llcp_sock_connect()权限提升漏洞”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-2021-43363

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43368

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43367

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43366

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43364

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43372

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43384

https://www.cnvd.org.cn/flaw/show/CNVD-2021-43385

5、D-Link DIR-2640-US 缓冲区溢出漏洞

D-Link DIR-2640-US 是一款智能 AC2600 大功率 Wi-Fi 千兆路由器。本周，D-Link DIR-2640-US 被披露存在缓冲区溢出漏洞。攻击者可通过反编译固件利用该漏洞访问

固件并提取敏感数据。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-2021-43376

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-2021-42144	ZOLL Defibrillator Dashboard 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zoll.com/products/data/hospital/defibrillator-dashboard-r-series
CNVD-2021-42313	ThroughTek P2P SDK 信息泄露漏洞	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.throughtek.com/about-throughteks-kalay-platform-security-mechanism/
CNVD-2021-42988	JerryScript 释放后重用漏洞（CNVD-2021-42988）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/jerryscript-project/jerryscript/issues/3748
CNVD-2021-43366	Linux kernel llcp_sock_bind()拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/
CNVD-2021-43371	SonicWall SonicOS 缓冲区溢出漏洞（CNVD-2021-43371）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0016
CNVD-2021-43379	Cisco DNA Center 证书验证漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-certvalid-USEj2CZk
CNVD-2021-43383	Google Android 权限提升漏洞（CNVD-2021-43383）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://source.android.com/security/bulletin/2021-05-01
CNVD-2021-43393	QNAP NAS 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://www.qnap.com/zh-tw/security-a

			dvisory/qsa-21-25
CNVD-2021-43403	Google Chrome 释放后重用漏洞（CNVD-2021-43403）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html
CNVD-2021-43001	JerryScript 堆缓冲区溢出漏洞（CNVD-2021-43001）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/jerryscript-project/jerryscript

小结：本周，Schneider Electric 产品被披露存在多个漏洞，攻击者可利用漏洞获取数据或实现远程代码执行。此外，SAP、OpenText、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问受限信息，通过恶意 GIF 文件利用该漏洞导致应用程序崩溃，在当前进程的上下文中执行代码，通过 Linux 内核的 perf_mmap_close()触发内存损坏，以触发拒绝服务并可能运行代码，生成非法的代码段，修改网络系统或组件的预期的执行控制流等。另外，D-Link DIR-2640-US 被披露存在缓冲区溢出漏洞。攻击者可通过反编译固件利用该漏洞访问固件并提取敏感数据。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、 bloofoxCMS 跨站请求伪造漏洞（CNVD-2021-43375）

验证描述

bloofoxCMS 是一款基于 PHP + MySQL 的免费开源 Web 内容管理系统。

bloofoxCMS 0.5.2.1 版存在跨站请求伪造漏洞。攻击者可利用该漏洞编辑任何文件内容。

验证信息

POC 链接：https://github.com/alexlang24/bloofoxCMS/issues/10

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-43375

信息提供者

华为技术有限公司

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. Windows 11 镜像和屏幕截图泄露

16 日，某开发者泄露了微软全新的 Windows 11 英文预览版。预览版界面改动很大，窗口采用圆角设计，开始菜单取消了动态磁贴，任务栏默认居中设计，跟之前取消的 Win10X 系统比较像。

参考链接：https://www.solidot.org/story?sid=68050

2. 1990 年代的移动加密算法被发现含有后门

德国波鸿鲁尔大学的研究人员与法国和挪威的同事合作发表了一篇论文，发现 1990 年代实现的移动手机加密算法 GEA-1 含有后门。GEA-1 仍然包含在最近几年发售的 Android 和 iOS 手机中。

参考链接：https://www.solidot.org/story?sid=68058

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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