国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 09 月 20 日-2021 年 09 月 26 日 **2021 年第 38 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 420 个，其中高危漏洞 128 个、中危漏洞 253 个、低危漏洞 39 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 314 个（占 75%），其中互联网上出现“WordPress Modern Events Calendar 远程代码执行漏洞、ToaruOS 权限提升漏洞”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原创漏洞总数 4843 个，与上周（5176 个）环比减少 6%。

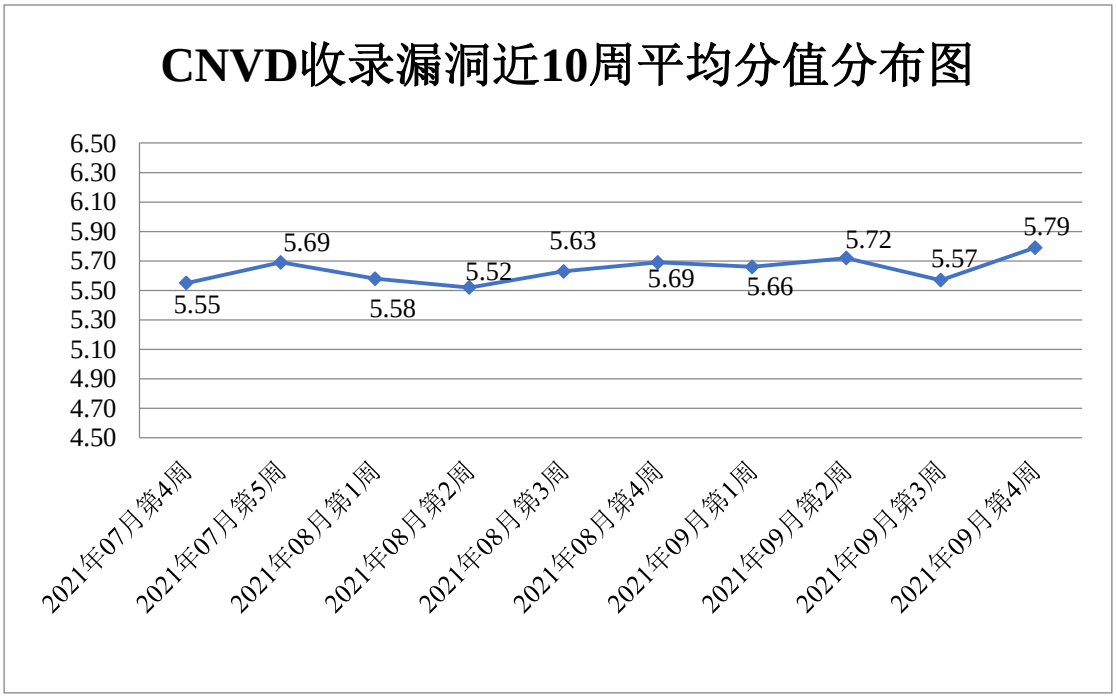

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 11 起，向基础电信企业通报漏洞事件 28 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 359 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 44 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 46 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：

淄博闪灵网络科技有限公司、中国电信集团有限公司、郑州维维信息技术有限公司、浙江大华技术股份有限公司、长沙冠讯网络科技有限公司、友讯电子设备（上海）有限公司、优酷信息技术（北京）有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、武汉小码联城科技有限公司、武汉天地伟业科技有限公司、微软（中国）有限公司、万洲电气股份有限公司、天津神舟通用数据技术有限公司、天津南大通用数据技术股份有限公司、太原公共交通控股（集团）有限公司、苏州国网电子科技有限公司、四创科技有限公司、世邦通信股份有限公司、沈阳明致软件有限公司、深圳市迅雷网络技术有限公司、深圳市吉祥腾达科技有限公司、深圳市共济科技股份有限公司、深圳市安佳威视信息技术有限公司、上海穆云智能科技有限公司、上海二三四五移动科技有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、三星（中国）投资有限公司、青岛全民网络科技有限公司、普联技术有限公司、内蒙古浩海商贸有限公司、零视技术（上海）有限公司、临沂市公共交通集团有限公司、金蝶软件（中国）有限公司、佳能（中国）有限公司、华硕电脑（上海）有限公司、湖南壹拾捌号网络技术有限公司、湖南建研信息技术股份有限公司、河南省新星科技有限公司、杭州九麒科技有限公司、杭州粉盟科技有限公司、杭州迪普科技股份有限公司、杭州博采网络科技股份有限公司、广州职迅信息科技有限公司、广州网易计算机系统有限公司、广州市奥威亚电子科技有限公司、广州齐博网络科技有限公司、广州南方卫星导航仪器有限公司、广州安网通信技术有限公司、成都市公共交通集团有限公司、成都飞鱼星科技股份有限公司、北京映翰通网络技术股份有限公司、北京亿赛通科技发展有限责任公司、北京网康科技有限公司、北京搜狐互联网信息服务有限公司、北京硕人时代科技股份有限公司、北京世纪超星信息技术发展有限责任公司、北京神州数码云科信息技术有限公司、北京企牛网络科技有限公司、北京派网软件有限公司、北京口袋时尚科技有限公司、北京华宇信息技术有限公司、北京多点在线科技有限公司、北京棣南新宇科技有限公司、安徽省科迅教育装备有限公司、帝国软件、施耐德（Schneider Electric）、百度安全应急响应中心、魅思视频系统、XnSoft、VMware,Inc.、The Apache Software Foundation、PHPMyWind、phpgurukul、Lexmark、kyan、Heybbs、Greatek、Eclipse、devolo、bluecms 和 AKCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、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、华为技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、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、河南灵创电子科技有限公司、安徽长泰科技有限公司、杭州海康威视数字技术股份有限公司、山东新潮信息技术有限公司、广东蓝爵网络安全技术股份有限公司、新疆海狼科技有限公司、北京安帝科技有限公司、江苏快页信息技术有限公司、浙江木链物联网科技有限公司、河南信安世纪科技有限公司、内蒙古洞明科技有限公司、重庆贝特计算机系统工程有限公司、京东云安全、泰山信息科技有限公司、山东泽鹿安全技术有限公司、北京惠而特科技有限公司、杭州迪普科技股份有限公司、内蒙古云科数据服务股份有限公司、北京远禾科技有限公司、福建省海峡信息技术有限公司、长春嘉诚信息技术股份有限公司、上海纽盾科技股份有限公司、浙江大华技术股份有限公司、平安银河实验室、北京天地和兴科技有限公司、中电长城网际系统应用有限公司、重庆都会信息科技有限公司、深圳市魔方安全科技有限公司、思而听网络科技有限公司、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 4843 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 3048 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）	2102	2102
北京天融信网络安全技术有限公司	500	4
上海交大	477	477
奇安信网神（补天平台）	469	469
北京神州绿盟科技有限公司	281	10
哈尔滨安天科技集团股份有限公司	212	0
北京数字观星科技有限公司	186	0
华为技术有限公司	158	0
新华三技术有限公司	102	0

北京启明星辰信息安全技术有限公司	97	1
恒安嘉新（北京）科技股份公司	91	0
北京奇虎科技有限公司	68	0
深信服科技股份有限公司	65	0
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	56	0
西安四叶草信息技术有限公司	48	48
南京联成科技发展股份有限公司	8	8
北京安信天行科技有限公司	2	2
北京长亭科技有限公司	1	1
山东云天安全技术有限公司	269	269
南京众智维信息科技有限公司	85	85
北京山石网科信息技术有限公司	81	81
联想全球安全实验室	78	0
河南灵创电子科技有限公司	59	59
安徽长泰科技有限公司	57	57
杭州海康威视数字技术股份有限公司	56	56
山东新潮信息技术有	47	47

限公司		
亚信科技（成都）有限公司	22	0
广东蓝爵网络安全技术股份有限公司	22	22
新疆海狼科技有限公司	21	21
北京安帝科技有限公司	21	21
中国电信股份有限公司网络安全产品运营中心	20	0
江苏快页信息技术有限公司	20	20
浙江木链物联网科技有限公司	19	19
河南信安世纪科技有限公司	19	19
内蒙古洞明科技有限公司	18	18
重庆贝特计算机系统工程有限公司	17	17
京东云安全	14	14
泰山信息科技有限公司	13	13
山东泽鹿安全技术有限公司	12	12
北京惠而特科技有限公司	11	11
杭州迪普科技股份有限公司	10	0
内蒙古云科数据服务股份有限公司	8	8
北京远禾科技有限公	6	6

司		
福建省海峡信息技术有限公司	6	6
长春嘉诚信息技术股份有限公司	6	6
上海纽盾科技股份有限公司	5	5
浙江大华技术股份有限公司	4	4
平安银河实验室	3	3
北京天地和兴科技有限公司	3	3
中电长城网际系统应用有限公司	2	2
重庆都会信息科技有限公司	2	2
深圳市魔方安全科技有限公司	2	2
思而听网络科技有限公司	2	2
北京机沃科技有限公司	1	1
CNCERT 河北分中心	18	18
CNCERT 西藏分中心	1	1
CNCERT 浙江分中心	1	1
个人	790	790
报送总计	6774	4843

本周漏洞按类型和厂商统计

本周，CNVD 收录了 420 个漏洞。WEB 应用 167 个，应用程序 148 个，网络设备（交换机、路由器等网络端设备）58 个，智能设备（物联网终端设备）22 个，安全产品 13 个，操作系统 12 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	167
应用程序	148
网络设备（交换机、路由器等网络端设备）	58
智能设备（物联网终端设备）	22
安全产品	13
操作系统	12

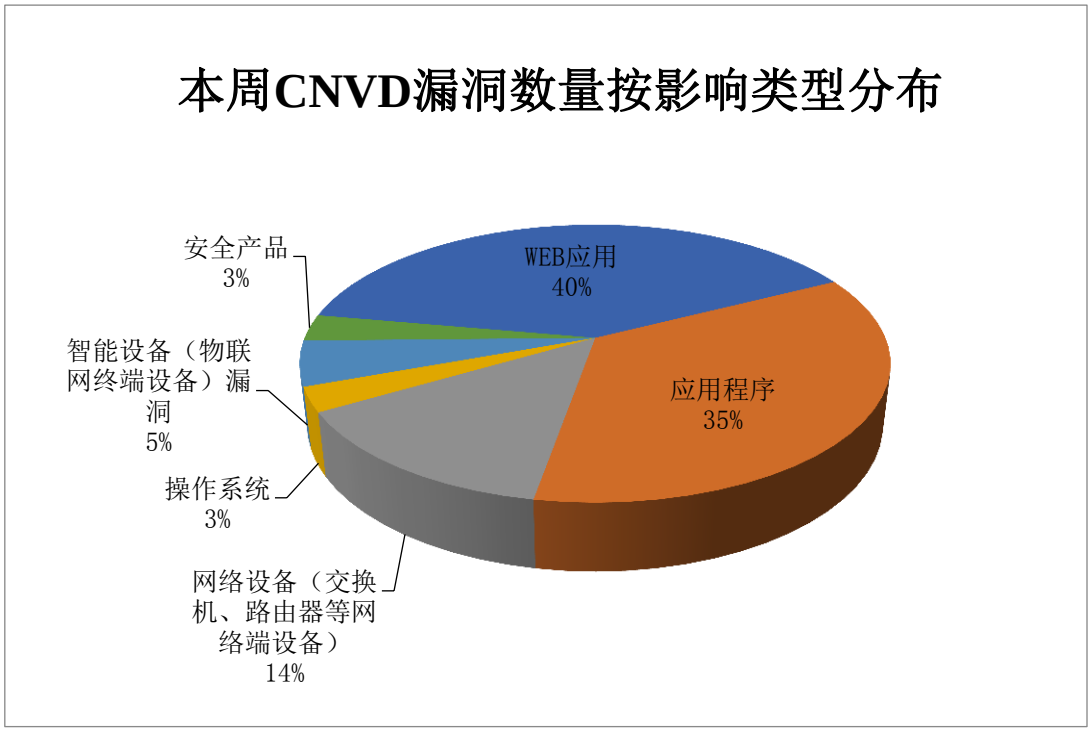

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SWFTools、Google、北京映翰通网络技术股份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	SWFTools	32	7%
2	Google	20	5%
3	北京映翰通网络技术股份有限公司	18	4%
4	Tuxera	17	4%
5	D-Link	16	4%
6	超级外卖 Super Cms	11	3%
7	Foxit	11	3%
8	Microsoft	9	2%
9	Adobe	8	2%
10	其他	278	66%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，24 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“ASUS RT-AX3000 拒绝服务漏洞、多款 Cisco SD-WAN 产品缓冲区溢出漏洞”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/

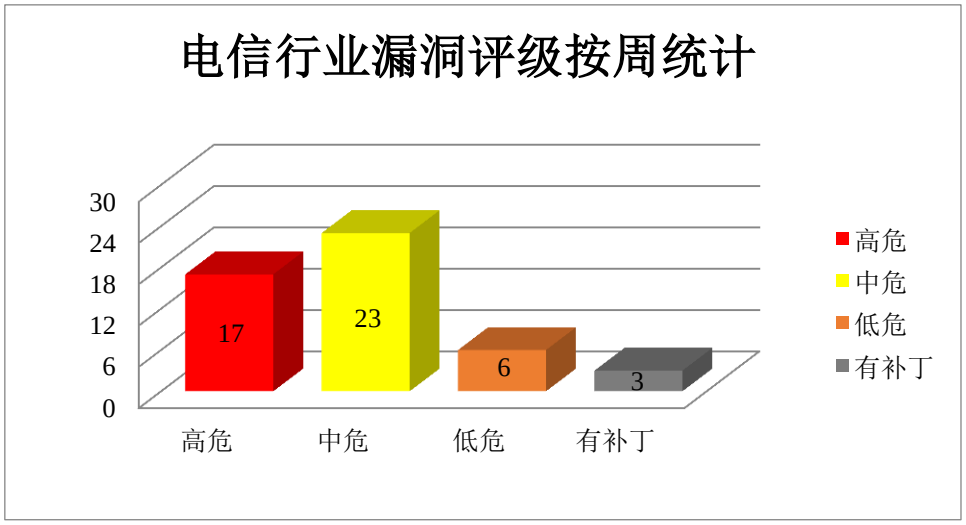

图 3 电信行业漏洞统计

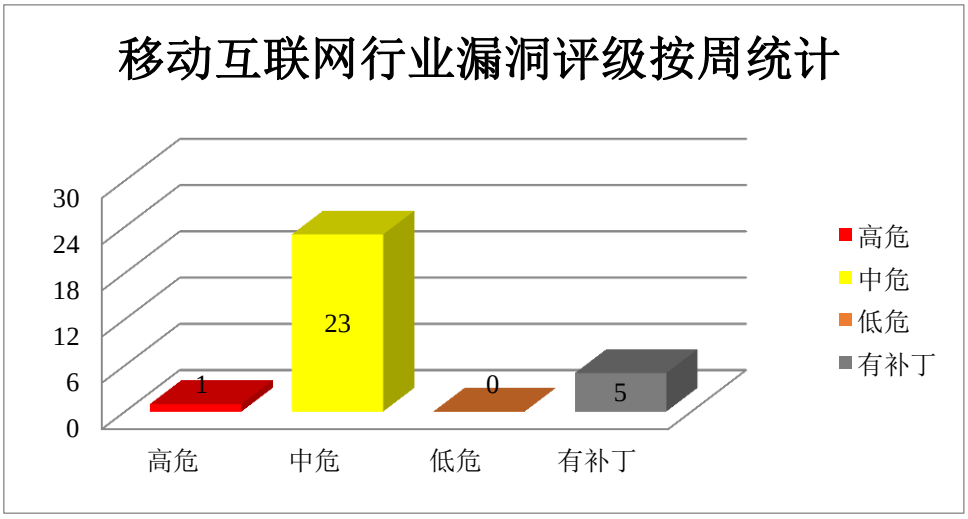

图 4 移动互联网行业漏洞统计

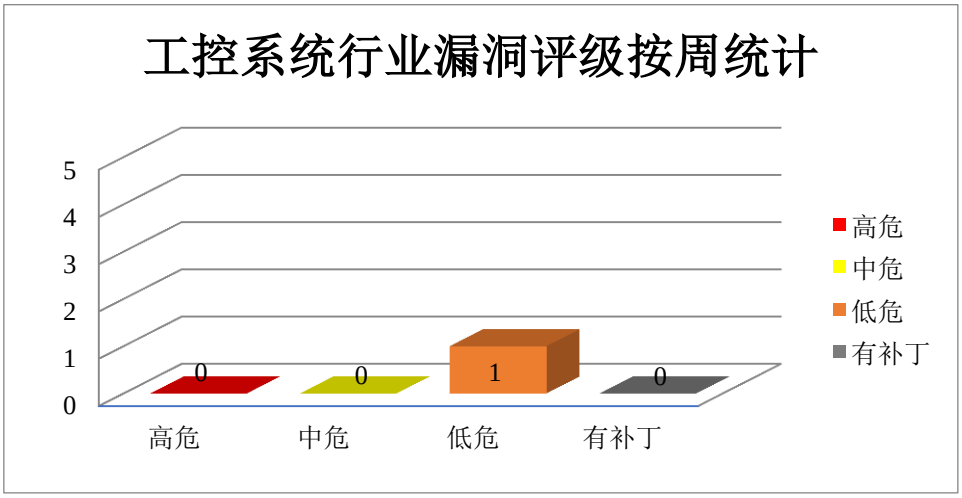

图 5 工控系统行业漏洞统计

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。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，绕过安全限制，在系统上执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Chrome libjpeg-turbo 信息泄露漏洞、Google Chrome Background Fetch API 安全绕过漏洞、Google Chrome Blink graphics 安全绕过漏洞、Google Chrome Tab Strip 代码执行漏洞、Google Chrome Performance Manager 代码执行漏洞、Google Chrome Offline 代码执行漏洞、Google Chrome WebGPU 代码执行漏洞、Google Chrome Navigation 安全绕过漏洞。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-2021-73414
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73421
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73426
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73425
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73424
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73430
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73429
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73428

2、 Adobe 产品安全漏洞

Adobe FrameMaker 是一款文档处理程序，用于编写和编辑包括结构化文档在内的

大型或复杂文档。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件系统，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Framemaker 越界写入漏洞（CNVD-2021-73434）、Adobe Framemaker 内存越界访问漏洞（CNVD-2021-73437、CNVD-2021-73436）、Adobe Framemaker 越界写入漏洞（CNVD-2021-73435）、Adobe Framemaker 释放后重用漏洞、Adobe Framemaker 越界读取漏洞（CNVD-2021-73440、CNVD-2021-73439、CNVD-2021-73438）。其中，“Adobe Framemaker 越界写入漏洞（CNVD-2021-73434）、Adobe Framemaker 内存越界访问漏洞（CNVD-2021-73437、CNVD-2021-73436）、Adobe Framemaker 越界写入漏洞（CNVD-2021-73435）” 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-2021-73434
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73437
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73436
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73435
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73441
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73440
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73439
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73438

3、 Microsoft 产品安全漏洞

Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞以提升的权限运行任意代码，从而可安装程序，查看、更改或删除数据，或创建具有完全用户权限的新帐户。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-73129、CNVD-2021-73128、CNVD-2021-73127、CNVD-2021-73132、CNVD-2021-73131、CNVD-2021-73130、CNVD-2021-73134、CNVD-2021-73133）。其中，“Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-73130、CNVD-2021-73134、CNVD-2021-73133）”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-2021-73129
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73128
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73127
https://www.cnvd.org.cn/flaw/show/CNVD-2021-73132

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73131

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73130

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73134

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73133

4、Tuxera 产品安全漏洞

Tuxera NTFS-3G 是芬兰 Tuxera 公司的一套开源的、跨平台的用于支持 NTFS 分区读写的驱动程序。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致缓冲区溢出，从而允许执行代码和提升权限等。

CNVD 收录的相关漏洞包括：Tuxera NTFS-3G 缓冲区溢出漏洞（CNVD-2021-72267、CNVD-2021-72266、CNVD-2021-72269、CNVD-2021-72268、CNVD-2021-72271、CNVD-2021-72272、CNVD-2021-72273、CNVD-2021-72275）。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-2021-72267

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72266

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72269

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72268

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72271

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72272

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72273

https://www.cnvd.org.cn/flaw/show/CNVD-2021-72275

5、Totolink A720R 堆栈溢出漏洞

Totolink A720R 是中国台湾吉翁电子（Totolink）公司的一款无线路由器。本周，Totolink A720R 被披露存在堆栈溢出漏洞。该漏洞源于软件中的 checkLoginUser 函数对数据的错误处理，攻击者可利用该漏洞造成拒绝服务（DOS）。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-2021-73657

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-2021-73206	FFmpeg 缓冲区溢出漏洞（CNVD-2021-73206）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://trac.ffmpeg.org/ticket/81

			90
CNVD-2021-73422	Google Chrome ChromeOS Networking 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html
CNVD-2021-73420	Google Chrome Compositing 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html
CNVD-2021-73431	Google Chrome Indexed DB API 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://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html
CNVD-2021-73653	ZOHO ManageEngine OpManager 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://www.manageengine.com/network-monitoring/help/read-me-complete.html#125203
CNVD-2021-73652	ASUS RT-AX3000 拒绝服务漏洞	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.asus.com/us/ASUSWRT/
CNVD-2021-73651	PHPMailer 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
CNVD-2021-73656	NukeViet SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/nukeviet/nukeviet/pull/2740/commits/05dfb9b4531f12944fe39556f58449b9a56241be
CNVD-2021-73655	Evolucare Ecsimaging 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.evolucare.com/en/?region=asi
CNVD-2021-73654	多款 Cisco SD-WAN 产品缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP

小结：本周，Google 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，绕过安全限制，在系统上执行任意代码或造成拒绝服务。此外，Adobe、Microsoft、Tuxera 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件系统，导致缓冲区溢出，执行任意代码，提升权限等。另外，Totolink A720R 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞造成拒绝服务（DOS）。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、WordPress Modern Events Calendar 远程代码执行漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress Modern Events Calendar 存在远程代码执行漏洞，攻击者可以利用该漏洞执行任意代码。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2021070157

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-73650

信息提供者

深信服科技股份有限公司

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. 海康威视摄像头存在远程代码执行漏洞

一个被跟踪为 CVE-2021-36260 的关键问题影响了 70 多个海康威视设备模型，并且可能允许攻击者接管它们。该漏洞是海康威视 IP 摄像机/NVR 固件中的一个未经身份验证的远程代码执行（RCE）漏洞。

参考链接：https://securityaffairs.co/wordpress/122474/hacking/hikvision-cve-2021-362

60-flaw.html

2. Apple 的 macOS Finder 中披露了一个新的零日漏洞

安全研究人员在 Apple 的 macOS Finder 中披露了一个新的零日漏洞，攻击者可以利用该漏洞在 Mac 上运行任意命令。

参考链接：https://securityaffairs.co/wordpress/122447/hacking/zero-day-macos.html

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