国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 10 月 11 日-2021 年 10 月 17 日　　2021 年第 41 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 159 个，其中高危漏洞 51 个、中危漏洞 92 个、低危漏洞 16 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 52 个（占 33%），其中互联网上出现“WordPress Social Warfare 远程代码执行漏洞（CNVD-2021-77611）、WordPress 插件 Current Book 'Book Title and Author field'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原创漏洞总数 5750 个，与上周合刊（9212 个）环比减少 38%。

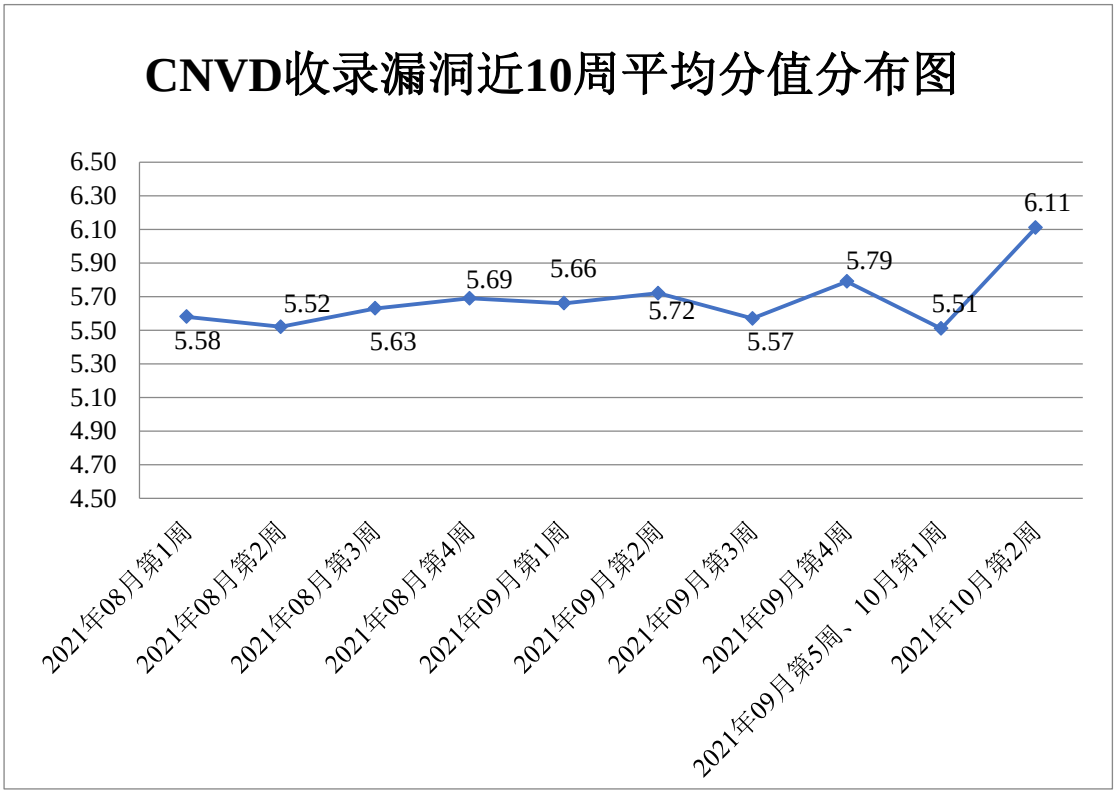

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 起，向基础电信企业通报漏洞事件 62 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 497 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 88 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 120 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：

重庆红杉软件有限公司、中国电信集团公司、郑州单点科技软件有限公司、长沙米拓信息技术有限公司、长沙冠讯网络科技有限公司、友讯电子设备（上海）有限公司、徐州亿优网架钢结构工程有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、新都（青岛）办公系统有限公司、西安兄弟信息科技有限公司、武汉中岩测控技术有限公司、武汉舜通智能科技有限公司、武汉光谷联合集团有限公司、微软（中国）有限公司、网件（北京）网络技术有限公司、天津市津购科技有限公司、唐桥科技（杭州）有限公司、太原迅易科技有限公司、松下电器（中国）有限公司、石家庄市征红网络科技有限公司、深圳市长鑫盛通科技有限公司、深圳市腾讯计算机系统有限公司、深圳市腾狐物联科技有限公司、深圳市美力高集团有限公司、深圳市美科星通信技术有限公司、深圳市脸萌科技有限公司、深圳市理才网信息技术有限公司、深圳市科曼医疗设备有限公司、深圳市巨龙科教网络有限公司、深圳市巨鼎医疗股份有限公司、深圳市皓峰通讯技术有限公司、上海纵之格科技有限公司、上海熠知电子科技有限公司、上海宜实信息科技有限公司、上海喜马拉雅科技有限公司、上海企炬网络科技有限公司、上海秒优供应链管理有限公司、上海肯特仪表股份有限公司、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、熵基科技股份有限公司、陕西硅峰网络科技有限公司、山东潍微科技股份有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、瑞斯康达科技股份有限公司、青岛东软载波智能电子有限公司、青岛艾玛信息技术有限公司、奇安信科技集团股份有限公司、南京怀宇科技有限公司、美国菲力尔公司、景腾多媒體股份有限公司、江西类友网络科技有限公司、济宁易搜信息科技有限公司、济南有人物联网技术有限公司、惠普贸易（上海）有限公司、华特数字科技有限公司、华平信息技术股份有限公司、河北南昊高新技术开发有限公司、杭州海康威视系统技术有限公司、杭州海康威视数字技术股份有限公司、杭州当虹科技股份有限公司、杭州贝腾科技有限公司、杭州安恒信息技术股份有限公司、哈尔滨伟成科技有限公司、广州领立斯网络科技有限公司、广州酷狗计算机科技有限公司、广州巨杉软件开发有限公司、广州安网通信技术有限公司、广西壮族自治区农村信用社联合社、广东卓锐软件有限公司、福建星网

锐捷通讯股份有限公司、福建四创软件有限公司、福建科立讯通信有限公司、福建福昕软件开发股份有限公司、东方博冠（北京）科技有限公司、大唐电信科技股份有限公司、成都青软青之软件有限公司、畅捷通信息技术股份有限公司、北京智邦国际软件技术有限公司、北京致远互联软件股份有限公司、北京云创联合科技有限公司、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、北京文网亿联科技有限公司、北京网御星云信息技术有限公司、北京网易有道计算机系统有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京搜狗信息服务有限公司、北京仁和汇智信息技术有限公司、北京清元优软科技有限公司、北京米尔伟业科技有限公司、北京昆仑纵横科技发展有限公司、北京酷我科技有限公司、北京凯特伟业科技有限公司、北京德惠众合信息技术有限公司、北京爱奇艺科技有限公司、百度安全应急响应中心、安徽鑫洲网络科技有限公司、安徽品格网络科技有限公司、安徽朋德信息科技有限公司、安徽吉尔信息科技有限公司、中央电视台、清华大学、无忧网络、信呼、巡云轻论坛、小说精品屋、梦想 CMS、MIP 建站系统、ZZCMS、XnSoft、WorldCast Systems、TuziCMS、The Apache Software Foundation、TaoCMS、SEMCMS、Overmax、Lexmark、KYOCERA、jfinal cms、Elefant CMS、DataGear、BlueCMS、Axis Communications AB、AO Kaspersky Lab、Adobe 和 ACD Systems International。

本周，CNVD 发布了《Microsoft 发布 2021 年 10 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6916

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、厦门服云信息科技有限公司、新华三技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。广东蓝爵网络安全技术股份有限公司、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、河南灵创电子科技有限公司、北京信联科汇科技有限公司、京东云安全、杭州海康威视数字技术股份有限公司、北京安帝科技有限公司、信联科技（南京）有限公司、杭州迪普科技股份有限公司、北京网御星云信息技术有限公司、安徽长泰科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京天地和兴科技有限公司、浙江木链物联网科技有限公司、内蒙古洞明科技有限公司、重庆都会信息科技有限公司、江苏快页信息技术有限公司、内蒙古云科数据服务股份有限公司、新疆海狼科技有限公司、北京远禾科技有限公司、平安银河实验室、云南南天电子信息产业股份有限公司、北京惠而特科技有限公司、北京机沃科技有限公司、奇安信-工控安全实验室、华泰人寿保险股份有限公司、银保信科技（北京）有限公司及其他个人白帽子向 CNVD 提交了 5750 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 3794 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）	3063	3063
奇安信网神（补天平台）	522	522
北京神州绿盟科技有限公司	315	11
哈尔滨安天科技集团股份有限公司	274	0
上海交大	209	209
厦门服云信息科技有限公司	195	0
新华三技术有限公司	186	2
华为技术有限公司	135	0
深信服科技股份有限公司	134	0
北京奇虎科技有限公司	108	0
北京天融信网络安全技术有限公司	107	8
恒安嘉新（北京）科技股份公司	87	0
国瑞数码零点实验室	59	0
北京启明星辰信息安全技术有限公司	51	4
北京数字观星科技有限公司	34	0
南京联成科技发展股份有限公司	20	20
卫士通信息产业股份有限公司	14	14
西安四叶草信息技术	10	10

有限公司		
北京知道创宇信息技术股份有限公司	4	0
杭州安恒信息技术股份有限公司	4	4
北京华顺信安科技有限公司	211	0
广东蓝爵网络安全技术股份有限公司	186	186
山东云天安全技术有限公司	163	163
联想全球安全实验室	144	0
南京众智维信息科技有限公司	97	97
河南灵创电子科技有限公司	95	95
北京信联科汇科技有限公司	79	79
京东云安全	43	43
杭州海康威视数字技术股份有限公司	41	41
北京安帝科技有限公司	33	33
亚信科技（成都）有限公司	30	0
信联科技（南京）有限公司	26	26
杭州迪普科技股份有限公司	19	6
北京网御星云信息技术有限公司	17	17
安徽长泰科技有限公司	13	13
北京云科安信科技有	11	11

限公司（Seraph 安全实验室）		
北京天地和兴科技有限公司	7	7
浙江木链物联网科技有限公司	6	6
内蒙古洞明科技有限公司	6	6
重庆都会信息科技有限公司	5	5
江苏快页信息技术有限公司	5	5
内蒙古云科数据服务股份有限公司	4	4
新疆海狼科技有限公司	3	3
北京远禾科技有限公司	3	3
平安银河实验室	3	3
云南南天电子信息产业股份有限公司	2	2
北京惠而特科技有限公司	2	2
北京机沃科技有限公司	1	1
奇安信-工控安全实验室	1	1
华泰人寿保险股份有限公司	1	1
银保信科技（北京）有限公司	1	1
CNCERT 宁夏分中心	6	6
CNCERT 云南分中心	1	1
个人	1016	1016

报送总计	7812	5750

本周漏洞按类型和厂商统计

本周，CNVD 收录了 159 个漏洞。应用程序 55 个，WEB 应用 34 个，操作系统 33 个，智能设备（物联网终端设备）21 个，网络设备（交换机、路由器等网络端设备）16 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
应用程序	55
WEB 应用	34
操作系统	33
智能设备（物联网终端设备）	21
网络设备（交换机、路由器等网络端设备）	16

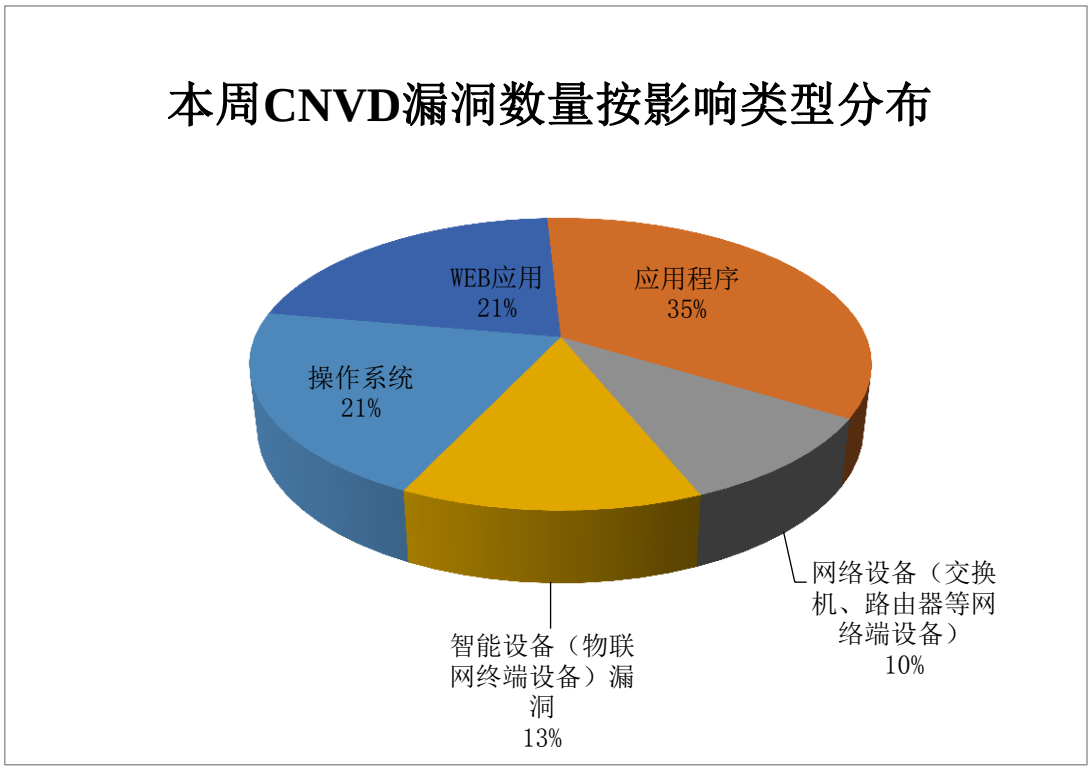

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SIEMENS、Brother、Microsoft 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	26	16%

2	Brother	17	11%
3	Microsoft	13	8%
4	PortlandLabs	12	8%
5	Google	12	8%
6	IrfanView	12	8%
7	Aruba Networks	9	6%
8	netscout	7	4%
9	Tecknodreams	7	4%
10	其他	44	27%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，12 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2021-77618）、Moxa EDR-G902 和 EDR-G903 堆栈缓冲区溢出漏洞、Siemens RUGGEDCOM ROX 设备拒绝服务漏洞”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/

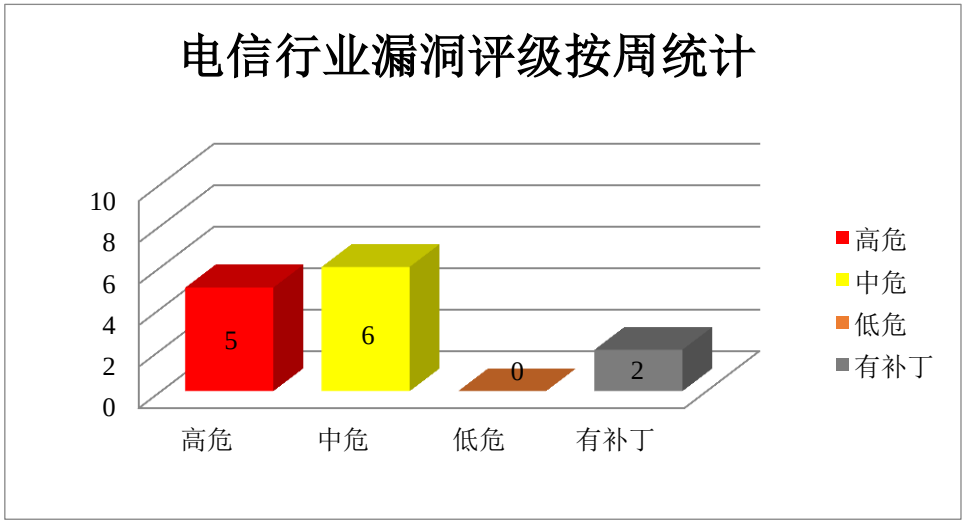

图 3 电信行业漏洞统计

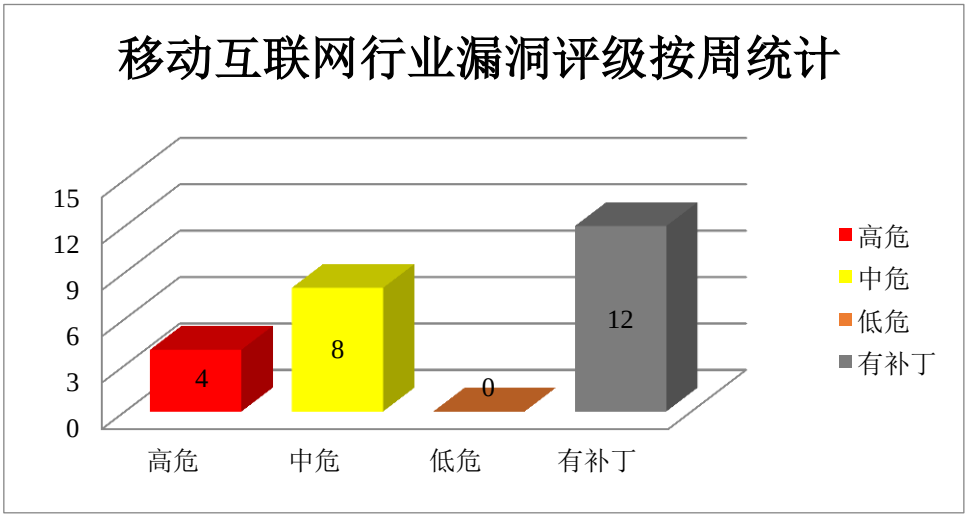

图 4 移动互联网行业漏洞统计

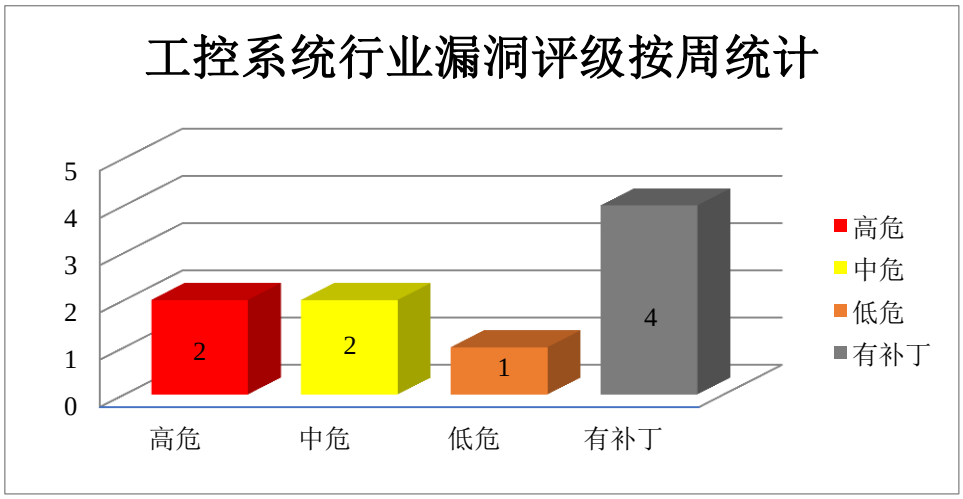

图 5 工控系统行业漏洞统计

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

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 代码执行漏洞（CNVD-2021-77613）、Google Android 权限提升漏洞（CNVD-2021-77616、CNVD-2021-77618、CNVD-2021-77617）、Google Android 信息泄露漏洞（CNVD-2021-77622、CNVD-2021-77621、CNVD-2021-77620、CNVD-2021-77624）。其中，“Google Android 代码执行漏洞（CNVD-2021-77613）、Google Android 权限提升漏洞（CNVD-2021-77616、CNVD-2021-776

18、CNVD-2021-77617）”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-2021-77613
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77616
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77618
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77617
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77622
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77621
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77620
https://www.cnvd.org.cn/flaw/show/CNVD-2021-77624

2、PortlandLabs 产品安全漏洞

PortlandLabs Concrete Cms 是美国 PortlandLabs 公司的一个面向团队的开源内容管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向服务器发送非预期的请求，导致客户端代码执行等。

CNVD 收录的相关漏洞包括：PortlandLabs Concrete CMS 路径遍历漏洞（CNVD-2021-76076、CNVD-2021-76078、CNVD-2021-76081、CNVD-2021-76089、CNVD-2021-76092）、PortlandLabs Concrete CMS 跨站脚本漏洞（CNVD-2021-76079、CNVD-2021-76088）、PortlandLabs Concrete CMS 跨站请求伪造漏洞（CNVD-2021-76080）。其中，“PortlandLabs Concrete CMS 路径遍历漏洞（CNVD-2021-76076、CNVD-2021-76092）”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-2021-76076
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76078
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76081
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76089
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76092
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76079
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76088
https://www.cnvd.org.cn/flaw/show/CNVD-2021-76080

3、Siemens 产品安全漏洞

Siemens Solid Edge 是一款 3D CAD、参数化特征和同步技术实体建模软件。SINEC NMS 是 Siemens 推出的用于监控和管理工业网络的网络管理系统。ROX-based VPN 端点和防火墙设备用于连接在恶劣环境中运行的设备，如电力设施变电站和交通控制柜。SINUMERIK CNC 为车间、车间和大型批量生产环境提供自动化解决方案。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，执行任意代码，造成拒

绝服务等。

CNVD 收录的相关漏洞包括：Siemens Solid Edge 释放后重用漏洞（CNVD-2021-75888、CNVD-2021-75891、CNVD-2021-75894）、Siemens Solid Edge 信息泄露漏洞、Siemens SINEC NMS 代码问题漏洞、Siemens SINEC NMS 任意文件删除漏洞、Siemens RUGGEDCOM ROX 设备拒绝服务漏洞、Siemens SINUMERIK Controllers 拒绝服务漏洞。其中，“Siemens SINEC NMS 代码问题漏洞、Siemens SINEC NMS 任意文件删除漏洞、Siemens RUGGEDCOM ROX 设备拒绝服务漏洞、Siemens SINUMERIK Controllers 拒绝服务漏洞”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-2021-75888

https://www.cnvd.org.cn/flaw/show/CNVD-2021-75891

https://www.cnvd.org.cn/flaw/show/CNVD-2021-75894

https://www.cnvd.org.cn/flaw/show/CNVD-2021-75893

https://www.cnvd.org.cn/flaw/show/CNVD-2021-77585

https://www.cnvd.org.cn/flaw/show/CNVD-2021-77596

https://www.cnvd.org.cn/flaw/show/CNVD-2021-77598

https://www.cnvd.org.cn/flaw/show/CNVD-2021-77605

4、 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多个漏洞，攻击者可利用漏洞提升权限，在受害者系统上执行任意代码，导致 DNS 服务无响应。

CNVD 收录的相关漏洞包括：Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-76462、CNVD-2021-76465、CNVD-2021-76464、CNVD-2021-76463）、Microsoft Windows 和 Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-76466）、Microsoft Windows Server 拒绝服务漏洞（CNVD-2021-76471）、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-76473、CNVD-2021-76472）。其中，“Microsoft Windows 和 Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-76466）” 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-2021-76462

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76465

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76464

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76463

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76466

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76471

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76473

https://www.cnvd.org.cn/flaw/show/CNVD-2021-76472

5、Irfanview 无限循环漏洞

IrfanView 是一款图片浏览器，它支持图片浏览、图片编辑、图片格式转换等。本周，IrfanView 被披露存在无限循环漏洞。攻击者可利用漏洞导致拒绝服务（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-2021-76100

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-2021-76084	Zoom Client 权限提升漏洞（CNVD-2021-76084）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cwe.mitre.org/data/definitions/379.html
CNVD-2021-77602	Aruba Operating System 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.arubanetworks.com/support-services/security-bulletins/
CNVD-2021-76082	ZOHO ManageEngine AD Manager Plus 代码执行漏洞	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.manageengine.com/products/ad-manager/release-notes.html#7111
CNVD-2021-76103	IrfanView WPG plugin 越界读取漏洞	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://www.irfanview.com/plugins.htm
CNVD-2021-77600	Aruba Operating System 命令注入漏洞（CNVD-2021-77600）	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://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-668/
CNVD-2021-76108	Moxa EDR-G902 和 EDR-G903 堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.moxa.com/en/support/support/security-advisory/edr-g902-g903-series-secure-routers-vulnerabilities

CNVD-2021-76794	Tecknodreams SapphireIMS 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.sapphireims.com/terms/
CNVD-2021-77595	Siemens SINEC NMS 路径遍历漏洞（CNVD-2021-77595）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-163251.pdf
CNVD-2021-77604	Aruba Operating System 跨站请求伪造漏洞	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://www.arubanetworks.com/support-services/security-bulletins/
CNVD-2021-77587	Siemens SINEC NMS SQL 注入漏洞（CNVD-2021-77587）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-163251.pdf

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，提升权限，执行任意代码。此外，PortlandLabs、Siemens、Microsoft 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，提升权限，执行任意代码，造成拒绝服务等。另外，Irfanview 被披露存在无限循环漏洞。攻击者可利用漏洞导致拒绝服务（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 Social Warfare 远程代码执行漏洞（CNVD-2021-77611）

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 Social Warfare 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-2021070167

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-77611

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. Windows PC 推出安全补丁，修复多个零日漏洞

2021 年 10 月 12 日，微软推出 Windows PC 安全补丁，包括 Windows PC 和其他软件一共有 71 个漏洞，其中还有一个被积极利用的特权提升漏洞，可以与远程代码执行漏洞一起被利用。

参考链接：https://thehackernews.com/2021/10/update-your-windows-pcs-immediately-to.html

2. OpenOffice 和 LibreOffice 发现数字签名漏洞

OpenOffice 和 LibreOffice 存在数字签名漏洞，攻击者可利用漏洞来修改文档，目前 LibreOffice 和 OpenOffice 已经完成了软件更新，修复了这些漏洞。

参考链接：https://thehackernews.com/2021/10/digital-signature-spoofing-flaws.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