国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 07 月 05 日-2021 年 07 月 11 日　　2021 年第 27 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 541 个，其中高危漏洞 129 个、中危漏洞 352 个、低危漏洞 60 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 234 个（占 43%），其中互联网上出现“Monstra CMS 跨站脚本漏洞（CNVD-2021-49037）、phpList 身份验证绕过漏洞”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 4773 个，与上周（3505 个）环比增加 36%。

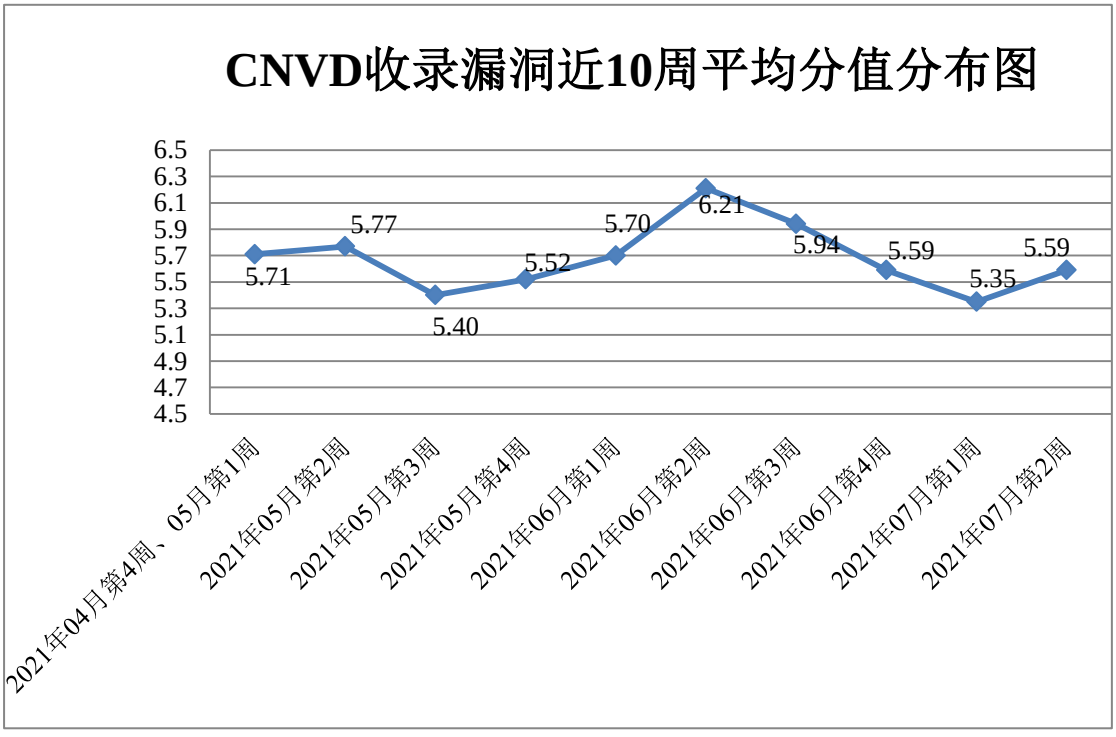

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 19 起，向基础电信企业通报漏洞事件 40 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 440 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 45 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 44 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、珠海全志科技股份有限公司、珠海玖时光科技有限公司、珠海金山办公软件有限公司、重庆软狐信息技术有限公司、重庆泛普软件有限公司、中通云仓科技有限公司、中科博华信息科技有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、运城市盘石网络科技有限公司、用友网络科技股份有限公司、新都（青岛）办公设备有限公司、夏普商贸（中国）有限公司、西安紫云羚网络科技有限责任公司、西安润格电子科技有限公司、武汉舜通智能科技有限公司、潍坊家园驿站电子技术有限公司、微软（中国）有限公司、唐山市柳林自动化设备有限公司、苏州思迪信息技术有限公司、苏州梦图地理信息系统有限责任公司、苏州科达科技股份有限公司、石家庄和嘉科技有限公司、神州数码集团股份有限公司、深圳维盟科技股份有限公司、深圳市智志高新科技开发有限公司、深圳市亿联网络科技有限公司、深圳市网域科技股份有限公司、深圳市万网博通投资管理有限合伙企业、深圳市深日科技有限公司、深圳市塞伯罗斯科技有限公司、深圳市领空技术有限公司、深圳市蓝凌软件股份有限公司、深圳市锟锔科技有限公司、深圳市吉祥腾达科技有限公司、深圳前海华夏智信数据科技有限公司、上海焱凤信息技术有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、陕西途悠悠供应链管理有限公司、厦门市灵鹿谷科技有限公司、三星（中国）投资有限公司、全讯汇聚网络科技（北京）有限公司、青岛万物一体网络科技有限公司、青岛东软载波智能电子有限公司、普联技术有限公司、零视技术（上海）有限公司、力天创见科技（深圳）有限公司、理光（中国）投资有限公司、廊坊市极致网络科技有限公司、蓝盾信息安全技术股份有限公司、魁网科技（重庆）有限公司、惠普贸易（上海）有限公司、洪湖尔创网联信息技术有限公司、杭州三汇信息工程有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、海南赞赞网络科技有限公司、桂林崇胜网络科技有限公司、广州图创计算机软件开发有限公司、广州市公共交通集团有限公司、广州市佰维网络科技有限公司、广州酷狗计算机科技有限公司、广州红帆科技有限公司、谷歌公司、福建科立讯通信有限公司、东营市公交公司、东莞市智跃软件科技有限公司、戴尔（中国）有限公司、成都星锐蓝海网络科技有限公司 、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、北京云科安信科技有限公司、北京星网锐捷网络技术有限公司、北京五八信息技术有限公司、北京万维盈创科技发展有限公司、北京神州数码云科信息技术有限公

司、北京国炬信息技术有限公司、北京东华原医疗设备有限责任公司、北京东方通科技股份有限公司、北京棣南新宇科技有限公司、北京博乐虎科技有限公司、北京博华信智科技股份有限公司、北京百卓网络技术有限公司、爱普生（中国）有限公司、互联网域名系统北京市工程研究中心、成都零起飞网络、深圳好生意网络工作室、百度安全应急响应中心、鱼跃 CMS、梦想 CMS、海洋 CMS、TaoLer 社区系统、C-Lodop 打印、ZengCMS、The Apache Software Foundation、TaoLer、SSYCMS、SeaCMS、RPCMS、noneCms、NETGEAR、MyuCMS、MuYuCMS、Lexmark、Joomla!、DzzOffice、CIRCONTROL、CatfishCMS、BlueCMS、Axis Communications AB 和 Guthrie CAD/GIS Software Pty Ltd.。

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、哈尔滨安天科技集团股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、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。山东云天安全技术有限公司、杭州木链物联网科技有限公司、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、山东新潮信息技术有限公司、山东泽鹿安全技术有限公司、江西省掌控者信息安全技术有限公司、长春嘉诚信息技术股份有限公司、河南灵创电子科技有限公司、北京华云安信息技术有限公司、武汉明嘉信信息安全检测评估有限公司、重庆都会信息科技有限公司、广东蓝爵网络安全技术股份有限公司、北京天地和兴科技有限公司、中国电信股份有限公司网络安全产品运营中心、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、北京安帝科技有限公司、北京远禾科技有限公司、南京树安信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、星云博创科技有限公司、贵州多彩宝互联网服务有限公司、北京顶象技术有限公司、四川哨兵信息科技有限公司、浙江御安信息技术有限公司、广州安亿信软件科技有限公司、广州易东信息安全技术有限公司、杰润鸿远（北京）科技有限公司、京东云安全、武汉绿色网络信息服务有限责任公司、北京墨云科技有限公司、广州百蕴启辰科技有限公司、江苏省信息安全测评中心、山东道普测评技术有限公司、深圳市魔方安全科技有限公司、中国工商银行、四川赛闯检测股份有限公司及其他个人白帽子向 CNVD 提交了 4773 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 2204 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）	1342	1342
奇安信网神（补天平台）	475	475

北京天融信网络安全技术有限公司	433	6
上海交大	387	387
哈尔滨安天科技集团股份有限公司	239	0
北京神州绿盟科技有限公司	223	7
新华三技术有限公司	164	0
北京数字观星科技有限公司	143	0
恒安嘉新（北京）科技股份公司	129	0
华为技术有限公司	125	0
深信服科技股份有限公司	124	2
北京启明星辰信息安全技术有限公司	93	35
国瑞数码零点实验室	57	0
卫士通信息产业股份有限公司	31	1
北京奇虎科技有限公司	7	7
北京知道创宇信息技术有限公司	3	0
南京联成科技发展股	2	2

份有限公司		
内蒙古奥创科技有限公司	2	2
山东云天安全技术有限公司	465	465
联想全球安全实验室	264	0
杭州木链物联网科技有限公司	239	239
北京信联科汇科技有限公司	187	187
北京山石网科信息技术有限公司	71	71
山东新潮信息技术有限公司	49	49
山东泽鹿安全技术有限公司	37	37
江西省掌控者信息安全技术有限公司	33	33
长春嘉诚信息技术股份有限公司	32	32
河南灵创电子科技有限公司	30	30
北京华云安信息技术有限公司	28	28
武汉明嘉信信息安全检测评估有限公司	28	28
重庆都会信息科技有限公司	26	26
广东蓝爵网络安全技术股份有限公司	24	24
北京天地和兴科技有限公司	21	21
中国电信股份有限公司网络安全产品运营	20	0

中心		
河南信安世纪科技有限公司	13	13
杭州迪普科技股份有限公司	13	0
北京安帝科技有限公司	9	9
北京远禾科技有限公司	8	8
南京树安信息技术有限公司	7	7
北京云科安信科技有限公司（Seraph 安全实验室）	6	6
星云博创科技有限公司	5	5
贵州多彩宝互联网服务有限公司	4	4
北京顶象技术有限公司	3	3
四川哨兵信息科技有限公司	3	3
浙江御安信息技术有限公司	3	3
广州安亿信软件科技有限公司	2	2
广州易东信息安全技术有限公司	2	2
杰润鸿远（北京）科技有限公司	2	2
京东云安全	2	2
武汉绿色网络信息服务有限责任公司	2	2
北京墨云科技有限公	1	1

司		
广州百蕴启辰科技有限公司	1	1
江苏省信息安全测评中心	1	1
山东道普测评技术有限公司	1	1
深圳市魔方安全科技有限公司	1	1
中国工商银行	1	1
四川赛闯检测股份有限公司	1	1
CNCERT 贵州分中心	6	6
CNCERT 宁夏分中心	2	2
CNCERT 四川分中心	2	2
CNCERT 山东分中心	1	1
个人	1148	1148
报送总计	6783	4773

本周漏洞按类型和厂商统计

本周，CNVD 收录了 541 个漏洞。应用程序 254 个，WEB 应用 168 个，网络设备（交换机、路由器等网络端设备）55 个，智能设备（物联网终端设备）30 个，操作系统 27 个，安全产品 6 个，数据库 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
应用程序	254
WEB 应用	168
网络设备（交换机、路由器等网络端设备）	55
智能设备（物联网终端设备）	30
操作系统	27
安全产品	6
数据库	1

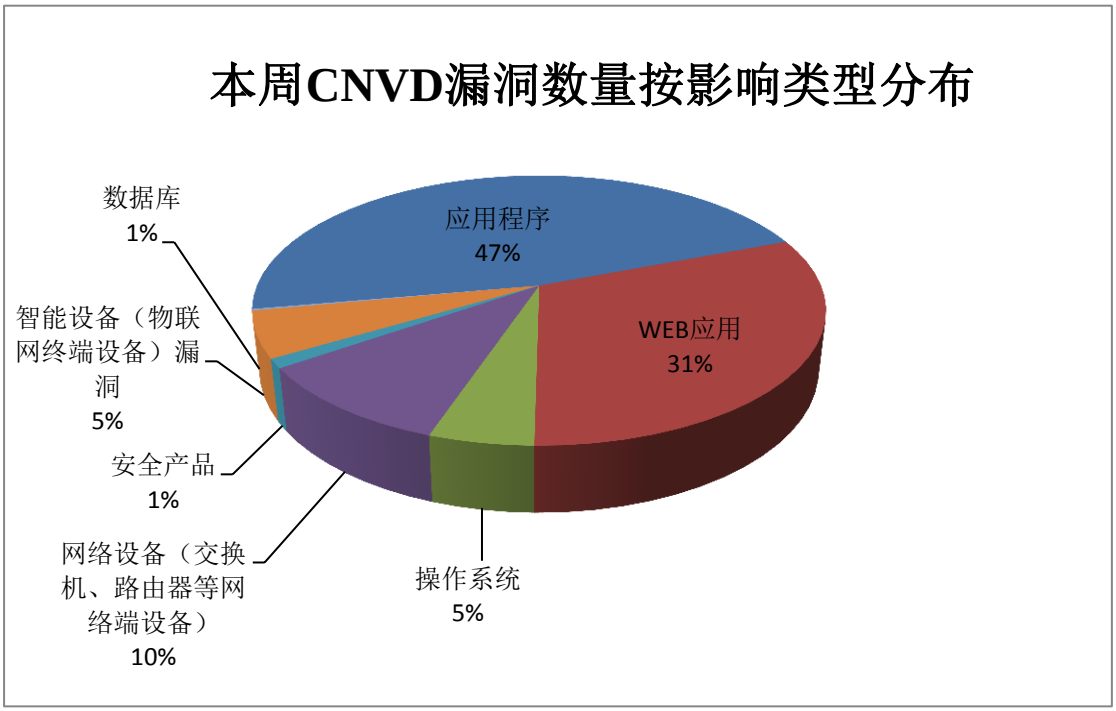

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、QSAN 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	Adobe	30	6%
2	Microsoft	27	5%
3	QSAN	19	4%
4	Google	18	3%
5	深圳市腾讯计算机系统有限公司	16	3%
6	北京棣南新宇科技有限公司	15	3%
7	SAP	14	2%
8	phpList	13	2%
9	mozilla	12	2%
10	其他	377	70%

本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，19 个移动互联网行业漏洞，22 个工控行业漏洞（如下图所示）。其中，“多款 NETGEAR 产品操作系统命令注入漏洞（CNVD-2021-48926）、Weidmueller Industrial WLAN devices 操作系统命令注入漏洞（CNVD-2021-48131）”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/

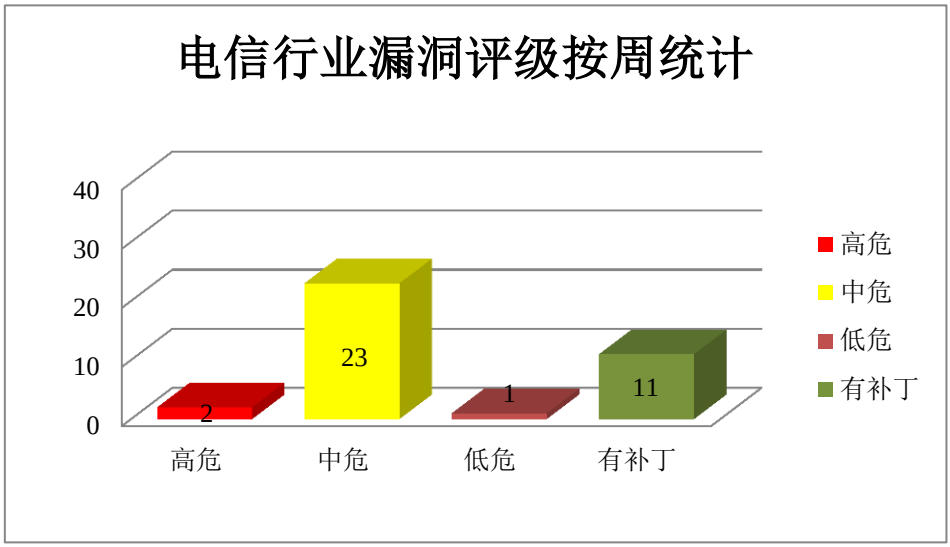

图 3 电信行业漏洞统计

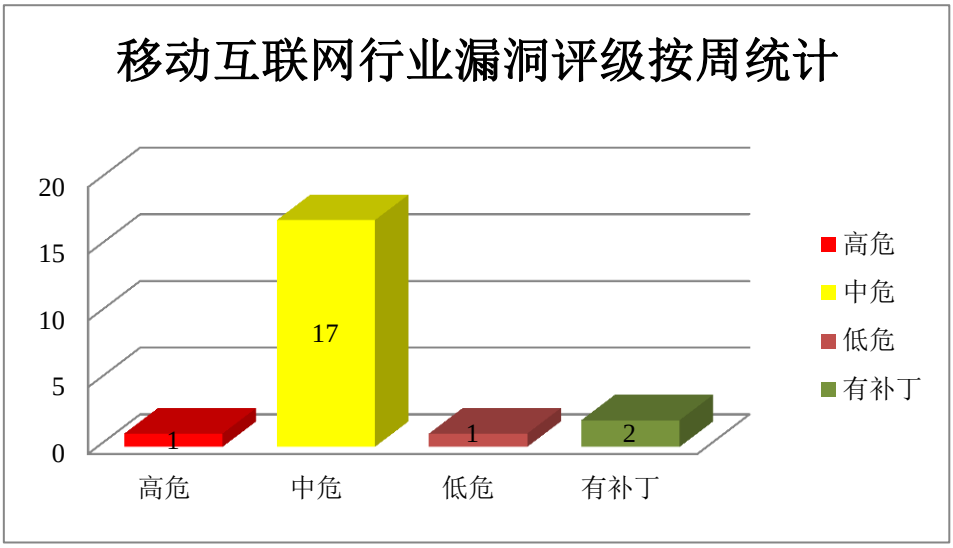

图 4 移动互联网行业漏洞统计

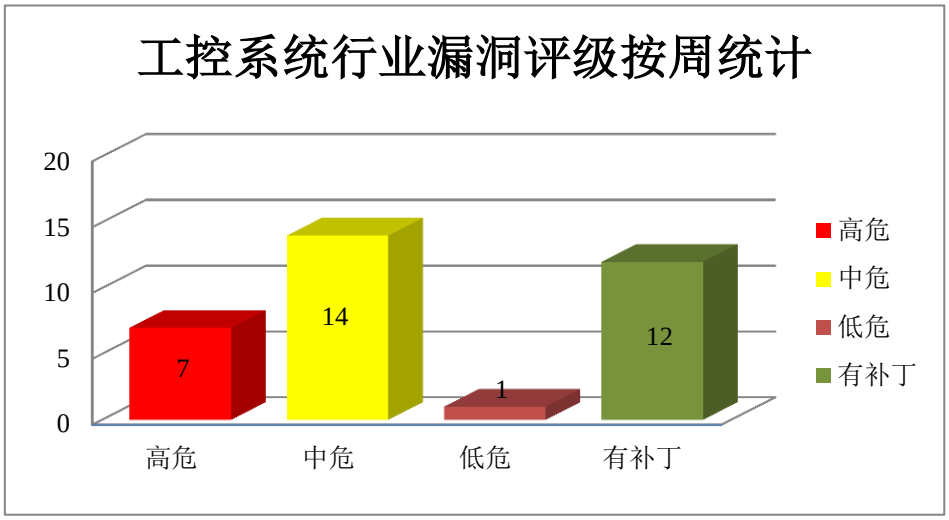

图 5 工控系统行业漏洞统计

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、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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制数据包导致系统崩溃，将明文命令插入网络上的加密 SMTP 会话等。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS for ABAP 内存破坏漏洞（CNVD-2021-47708、CNVD-2021-47707、CNVD-2021-47706、CNVD-2021-47710、CNVD-2021-47709）、SAP NetWeaver AS ABAP 命令注入漏洞、SAP NetWeaver ABAP Server and ABAP Platform 内存破坏漏洞（CNVD-2021-47715、CNVD-2021-47716）。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-2021-47708

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47707

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47706

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47711

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47710

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47709

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47716

https://www.cnvd.org.cn/flaw/show/CNVD-2021-47715

2、Microsoft 产品安全漏洞

Windows Print Spooler 是 Windows 的打印机后台处理程序。Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，导致应用程序崩溃或以应用程序上下文执行任意代码，对特定的 api 发送精心构造的数据远程执行命令，提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Windows Print Spooler 代码执行漏洞、Microsoft Windows Print Spooler 权限提升漏洞、Microsoft SharePoint 远程代码执行漏洞（CNVD-2021-48898、CNVD-2021-48891、CNVD-2021-48896、CNVD-2021-48893、CNVD-2021-48888）、Microsoft SharePoint 权限提升漏洞（CNVD-2021-48897）。其中，“Microsoft Windows Print Spooler 代码执行漏洞、Microsoft Windows Print Spooler 权限提升漏洞、Microsoft SharePoint 远程代码执行漏洞（CNVD-2021-48898）”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-2021-48426
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48427
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48898
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48891
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48897
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48896
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48893
https://www.cnvd.org.cn/flaw/show/CNVD-2021-48888

3、NETGEAR 产品安全漏洞

NETGEAR D3600 等都是美国网件（NETGEAR）公司的产品。NETGEAR D3600 是一款无线调制解调器。NETGEAR D6000 是一款无线调制解调器。NETGEAR D6100 是一款无线调制解调器。NETGEAR R6100 是一款无线路由器。NETGEAR R6900 是一款无线路由器。NETGEAR D7000 是一款无线调制解调器。NETGEAR R7500 是一款无线路由器。NETGEAR D7800 是一款无线调制解调器。NETGEAR R7800 是一款无线路由器。NETGEAR R9000 是一款无线路由器。NETGEAR M4300-28G 等都是美国网件（NETGEAR）公司的一款网管型交换机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞缓冲区溢出或堆溢出，执行非法操作系统命令等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-48928、CNVD-2021-48927、CNVD-2021-48925、CNVD-2021-48930、CNVD-2021-48929、CNVD-2021-48934）、多款 NETGEAR 产品操作系统命令注入漏洞（CNVD-2021-48926、CNVD-2021-48931）。其中，“多款 NETGEAR 产品操作系统命令注入漏洞（CNV

D-2021-48926）”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-2021-48928

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48927

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48926

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48925

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48931

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48930

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48929

https://www.cnvd.org.cn/flaw/show/CNVD-2021-48934

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃取受害者基于 Cookie 的身份验证凭据，授予 web 内容的其他特权，执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Thunderbird 代码问题漏洞（CNVD-2021-49128）、Mozilla Firefox 跨站脚本漏洞（CNVD-2021-49131）、多款 Mozilla 产品输入验证错误漏洞、多款 Mozilla 产品权限提升漏洞（CNVD-2021-49135）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2021-49133）、多款 Mozilla 产品资源管理错误漏洞（CNVD-2021-49138）、多款 Mozilla 产品数据伪造问题漏洞（CNVD-2021-49136）、多款 Mozilla 产品缓冲区溢出漏洞（CNVD-2021-49139）。其中，“多款 Mozilla 产品资源管理错误漏洞（CNVD-2021-49138）”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-2021-49128

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49131

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49130

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49135

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49133

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49138

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49136

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49139

5、QSAN Storage Manager 操作系统命令注入漏洞

QSAN Storage Manager 是广盛科技股份有限公司(QSAN)的一个 NAS 操作系统。本周，QSAN Storage Manager 被披露存在命令注入漏洞。攻击者可利用该漏洞执行任意命令。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-2021-48917

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-2021-47381	Prosodical Thoughts Prosody 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blog.prosody.im/prosody-0.11.9-released/
CNVD-2021-47637	Tenable Network Security Nessus 权限提升漏洞（CNVD-2021-47637）	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://zh-cn.tenable.com/security/tns-2021-07?tns_redirect=true
CNVD-2021-47642	Narou 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/whiteleaf7/narou/blob/develop/ChangeLog.md#380-20210627
CNVD-2021-47645	Securepoint SSL VPN Client 访问控制错误漏洞	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/Securepoint/openvpn-client/security/advisories/GHSA-v8p8-4w8f-qh34
CNVD-2021-48131	Weidmueller Industrial WLAN devices 操作系统命令注入漏洞（CNVD-2021-48131）	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.weidmueller.com/int/index.jsp
CNVD-2021-48845	PhpList 身份验证绕过漏洞（CNVD-2021-48845）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/phpList/phplist3
CNVD-2021-48852	Citrix SD-WAN Center 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://support.citrix.com/article/CTX285061
CNVD-2021-48879	Navigate CMS SQL 注入漏洞	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://github.com/NavigateCMS/Navigate-CMS/commit/d459b1d151350b401236e0a7f746c82a8fa80562
CNVD-2021-	Craft CMS 远程代码执行漏	高	目前厂商已发布升级补丁以修复漏

48877	洞		洞，详情请关注厂商主页：https://github.com/craftcms/cms/blob/develop/CHANGELOG.md#367---2021-02-23
CNVD-2021-48876	Apache Traffic Server 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://lists.apache.org/thread.html/ra1a41ff92a70d25bf576d7da2590575e8ff430393a3f4a0c34de4277%40%3Cusers.trafficserver.apache.org%3E

小结：本周，SAP 产品被披露存在多个漏洞，攻击者可利用漏洞发送特制数据包导致系统崩溃，将明文命令插入网络上的加密 SMTP 会话等。此外，Microsoft、NETGEAR、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，导致应用程序崩溃或以应用程序上下文执行任意代码，缓冲区溢出或堆溢出，执行非法操作系统命令。另外，QSAN Storage Manager 被披露存在命令注入漏洞。攻击者可利用漏洞执行任意命令。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、phpList 身份验证绕过漏洞

验证描述

phpList 是英国 phpList 公司的一套开源的新闻通讯和电子邮件营销软件。

phpList 3.5.0 版本存在身份验证绕过漏洞，该漏洞源于程序未正确处理开头为 0e 之后全部为数字字符的哈希值，远程攻击者可利用该漏洞绕过管理员账户的身份验证。

验证信息

POC 链接：https://www.exploit-db.com/exploits/47989

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-48846

信息提供者

阿里云计算有限公司

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. 微软：所有 Windows 版本的 PrintNightmare 漏洞已打补丁

Microsoft 已发布 KB5004948 紧急安全更新，以解决所有版本的 PrintNightmare 漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-versions/

2. WildPressure APT 小组被发现使用新恶意软件针对 Windows 和 macOS 平台

卡巴斯基的研究人员 8 日发现了 WildPressure APT 小组使用的一种新恶意软件，针对 Windows 和 macOS 平台。

参考链接：https://securityaffairs.co/wordpress/category/apt

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