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 13 日-2021 年 09 月 19 日　　2021 年第 37 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 392 个，其中高危漏洞 104 个、中危漏洞 239 个、低危漏洞 49 个。漏洞平均分值为 5.57。本周收录的漏洞中，涉及 0day 漏洞 288 个（占 73%），其中互联网上出现“TryGhost express-hbs 信息泄露漏洞、Tastylgniter 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 5176 个，与上周（6218 个）环比减少 17%。

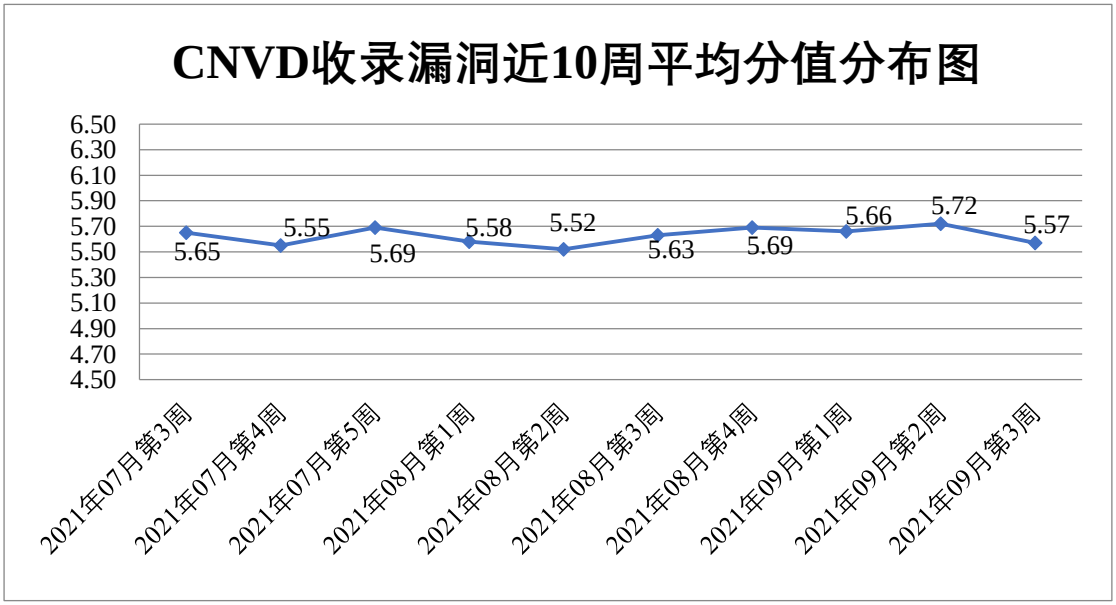

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 23 起，向基础电信企业通报漏洞事件 36 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 553 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 59 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 40 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、珠海金山办公软件有限公司、重庆光之际软件科技有限公司、中煤（西安）地下空间科技发展有限公司、中国电信集团公司、中电鸿信信息科技有限公司、致得科创软件（北京）有限公司、知和环保科技有限公司、支付宝（杭州）信息技术有限公司、镇江周易科技信息有限公司、浙江万方软件有限公司、浙江禾匠信息科技有限公司、浙江大华技术股份有限公司、云校（北京）科技有限公司、云从科技集团股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、新翔软件科技有限公司、新天科技股份有限公司、小米科技有限责任公司、祥崴電子股份有限公司、西门子（中国）有限公司、西安知先信息技术有限公司、西安新软信息科技有限公司、武汉江民网安科技有限公司、卫宁健康科技集团股份有限公司、幃翔精密股份有限公司、微软（中国）有限公司、网旭科技有限公司、万网博通科技有限公司、唐山市柳林自动化设备有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、四创科技有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、沈阳明致软件有限公司、深圳誉龙数字技术有限公司、深圳一正技术有限公司、深圳市网域科技技术有限公司、深圳市沙漠风网络科技有限公司、深圳市锐明技术股份有限公司、深圳市普燃计算机软件科技有限公司、深圳市模拟科技有限公司、深圳市麦斯杰网络有限公司、深圳市磊科实业有限公司、深圳市朗驰欣创科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市华域数安科技有限公司、深圳市和为顺网络技术有限公司、深圳市航顺芯片技术研发有限公司、深圳市电航科技发展有限公司、深圳前海金银星科技有限公司、深圳齐心好视通云计算有限公司、深圳华视美达信息技术有限公司、上海远丰信息科技（集团）有限公司、上海新网程信息技术股份有限公司、上海纽盾科技股份有限公司、上海汉得信息技术股份有限公司、上海安达通信息安全技术股份有限公司、熵基科技股份有限公司、山西合力思创科技有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、厦门科汛软件有限公司、人美新媒体科技（北京）有限公司、普联技术有限公司、宁波睿易教育科技股份有限公司、南通点酷网络科技有限公司、南京科远智慧科技集团股份有限公司、猎豹移动公司、联奕科技股份有限公司、理光（中国）投资有限公司、科大讯飞股份有限公司、精华教育科技股份有限公司、京瓷集团、江苏卓易信息科技股份有限公司、佳能（中国）有限公司、华特数字科技有限公司、华大半导体有限公司、湖南壹拾捌号网络技术有限公司、湖南青果软件有限公司、湖南建研信息技术股份有限公司、杭州涂鸦科技有限公司、杭州三汇数字信息

技术有限公司、杭州品茗安控信息技术股份有限公司、杭州海康威视数字技术股份有限公司、杭州冠航科技有限公司、杭州博联智能科技股份有限公司、广州纵道软件有限公司、广州网易计算机系统有限公司、广州市凝智科技有限公司、广州市国万电子科技有限公司、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、广州红帆科技有限公司、广州国微软件科技有限公司、广州鼎成信息科技有限公司、广东旭诚科技有限公司、谷歌公司、歌美斯有限公司、福州网钛软件科技有限公司、福州麦佳软件有限公司、福建三元达控股有限公司、东华软件股份公司、东莞市冬惊鱼网络科技有限公司、大连理工计算机控制工程有限公司、成都依能科技股份有限公司、北京众智创世科技有限公司、北京云创联合科技有限公司、北京映翰通网络技术股份有限公司、北京亿中邮信息技术有限公司、北京亿信华辰软件有限责任公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京通达信科科技有限公司、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、北京派网软件有限公司、北京良精志诚科技有限责任公司、北京金盘鹏图软件技术有限公司、北京宏业超世纪科技有限公司、北京和信康健康科技有限公司、北京和利时集团、北京海腾时代科技有限公司、北京多点在线科技有限公司、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、北京北大方正电子有限公司、北京爱奇艺科技有限公司、蚌埠依爱消防电子有限责任公司、傲拓科技股份有限公司、安徽中汇规划勘测设计研究院股份有限公司、安徽希望网络科技有限公司、ZIONCOM（香港）科技有限公司、小说精品屋、梦想 cms、零起飞工作室、帝国软件、ZCNCMS、XnSoft、The PHP Group、SEMCMS、phpaaCMS、PESCMS、Panabit、NETGEAR、muucmf、Lexmark、ICP DAS CO.、HDHCMS、HDCMS、FineCMS、Cisco、bluecms、Apple、Apache Software Foundation、akcms 和 Adobe。

本周，CNVD 发布了《Microsoft 发布 2021 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6846

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、北京奇虎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、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、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、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、内蒙古洞明科技有限公司、广东蓝爵网络安全技术股份有限公司、北京大学、

北京天地和兴科技有限公司、北京安华金和科技有限公司、安徽长泰科技有限公司、山东泽鹿安全技术有限公司、上海纽盾科技股份有限公司、重庆都会信息科技有限公司、浙江国利网安科技有限公司、内蒙古云科数据服务股份有限公司、河南信安世纪科技有限公司、北京远禾科技有限公司、京东云安全、中国烟草总公司湖北省公司、平安银河实验室、江苏快页信息技术有限公司、中电长城网际系统应用有限公司、广州安亿信软件科技有限公司、北京惠而特科技有限公司、南京树安信息技术有限公司、浙江木链物联网科技有限公司、浙江大华技术股份有限公司、山石网科通信技术股份有限公司、苏州叶安网络科技有限公司、北京科技大学、北京水木羽林科技有限公司、天讯瑞达通信技术有限公司、深圳市跨越新科技有限公司、西藏熙安信息技术有限责任公司、星云博创科技有限公司、深圳市魔方安全科技有限公司、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 5176 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 3093 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）	2195	2195
北京天融信网络安全技术有限公司	501	13
奇安信网神（补天平台）	498	498
上海交大	400	400
哈尔滨安天科技集团股份有限公司	301	0
北京神州绿盟科技有限公司	287	10
新华三技术有限公司	263	0
北京奇虎科技有限公司	228	0
深信服科技股份有限公司	168	0
华为技术有限公司	164	0
恒安嘉新(北京)科技股份公司	128	0
北京启明星辰信息安全技术有限公司	116	62

远江盛邦（北京）网络安全科技股份有限公司	61	61
天津市国瑞数码安全系统股份有限公司	59	0
亚信科技（成都）有限公司	31	0
南京联成科技发展股份有限公司	15	15
西安四叶草信息技术有限公司	7	7
杭州安恒信息技术股份有限公司	6	6
中兴通讯股份有限公司	5	5
北京安信天行科技有限公司	3	3
北京智游网安科技有限公司	1	1
山东云天安全技术有限公司	277	277
联想集团	178	0
河南灵创电子科技有限公司	133	133
南京众智维信息科技有限公司	125	125
北京信联科汇科技有限公司	75	75
北京山石网科信息技术有限公司	71	71
杭州海康威视数字技术股份有限公司	39	39
北京安帝科技有限公司	36	36
内蒙古洞明科技有限	36	36

公司		
西门子（中国）有限公司	34	0
广东蓝爵网络安全技术股份有限公司	29	29
北京大学	18	18
北京天地和兴科技有限公司	16	16
北京安华金和科技有限公司	16	16
杭州迪普科技股份有限公司	14	0
安徽长泰科技有限公司	14	14
山东泽鹿安全技术有限公司	14	14
上海纽盾科技股份有限公司	10	10
重庆都会信息科技有限公司	8	8
浙江国利网安科技有限公司	7	7
内蒙古云科数据服务股份有限公司	5	5
河南信安世纪科技有限公司	5	5
北京远禾科技有限公司	4	4
京东云安全	4	4
中国烟草总公司湖北省公司	3	3
平安银河实验室	3	3
江苏快页信息技术有限公司	3	3
中电长城网际系统应	3	3

用有限公司		
广州安亿信软件科技有限公司	2	2
北京惠而特科技有限公司	2	2
南京树安信息技术有限公司	2	2
浙江木链物联网科技有限公司	2	2
浙江大华技术股份有限公司	2	2
山石网科通信技术股份有限公司	1	1
苏州叶安网络科技有限公司	1	1
北京科技大学	1	1
北京水木羽林科技有限公司	1	1
天讯瑞达通信技术有限公司	1	1
深圳市跨越新科技有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
星云博创科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
北京机沃科技有限公司	1	1
CNCERT 河北分中心	7	7
CNCERT 四川分中心	5	5
CNCERT 贵州分中心	1	1
个人	913	913
报送总计	7563	5176

本周漏洞按类型和厂商统计

本周，CNVD 收录了 392 个漏洞。WEB 应用 174 个，应用程序 100 个，网络设备（交换机、路由器等网络端设备）71 个，操作系统 31 个，智能设备（物联网终端设备）9 个，安全产品 7 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	174
应用程序	100
网络设备（交换机、路由器等网络端设备）	71
操作系统	31
智能设备（物联网终端设备）	9
安全产品	7

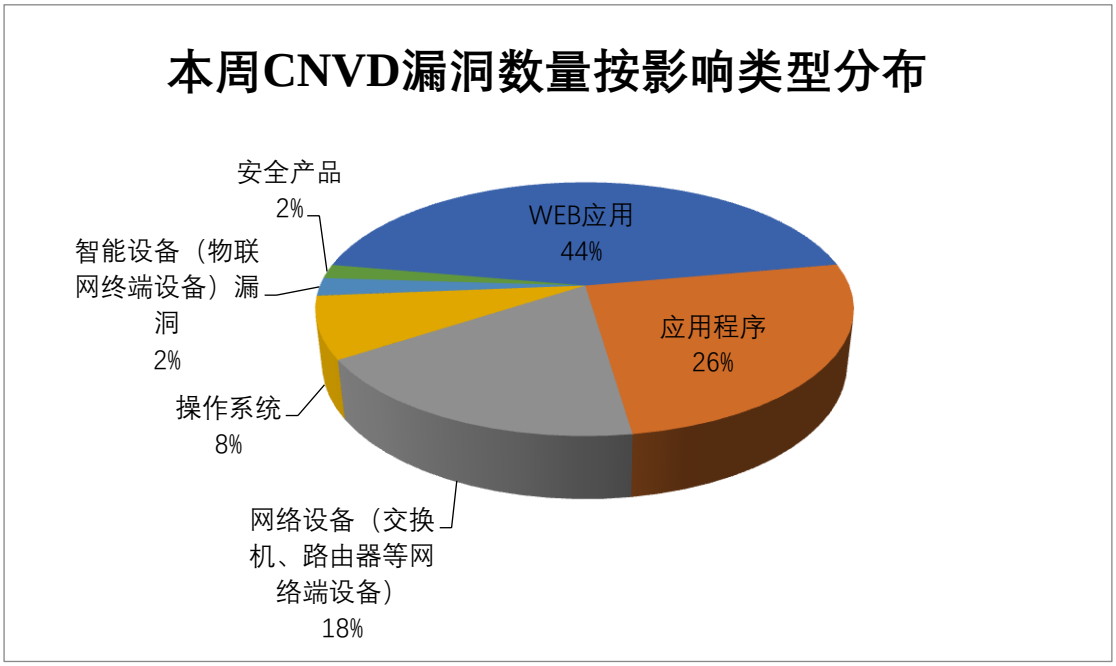

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、友讯电子设备（上海）有限公司、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	30	8%
2	友讯电子设备（上海）有限公司	29	7%
3	Microsoft	24	6%
4	The HDF Group	15	4%

5	WordPress	12	3%
6	IBM	11	3%
7	Mozilla	11	3%
8	北京映翰通网络技术股份有限公司	9	2%
9	广州本盈计算机科技有限公司	8	2%
10	其他	243	62%

本周行业漏洞收录情况

本周，CNVD 收录了 53 个电信行业漏洞，24 个移动互联网行业漏洞，19 个工控行业漏洞（如下图所示）。其中，“Aruba Networks ArubaOS 命令注入漏洞（CNVD-2021-71260）、Siemens SIPROTEC 5 relays 缓冲区溢出漏洞”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/

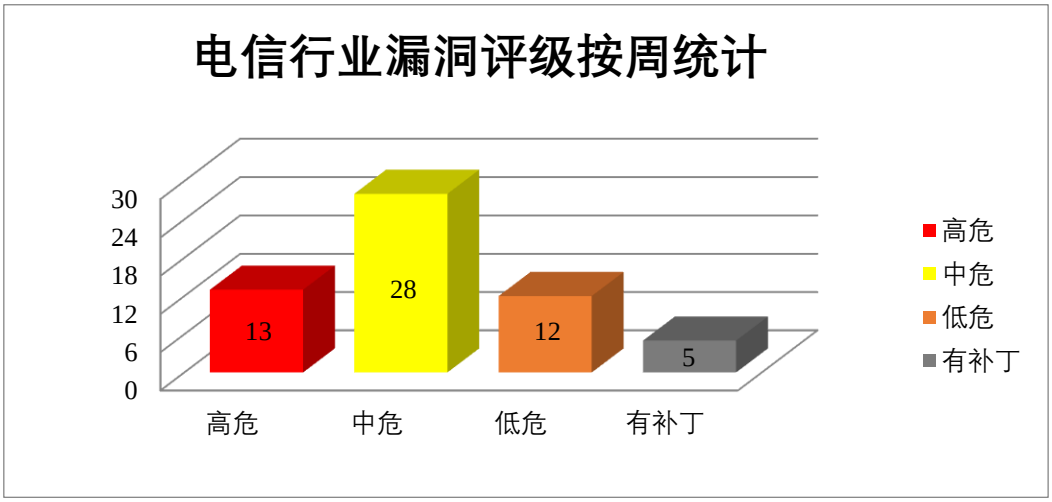

图 3 电信行业漏洞统计

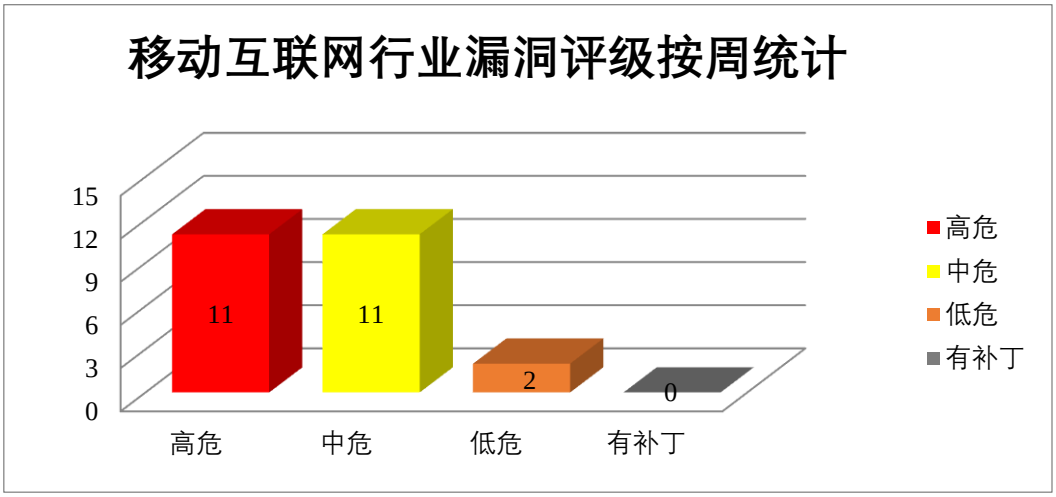

图 4 移动互联网行业漏洞统计

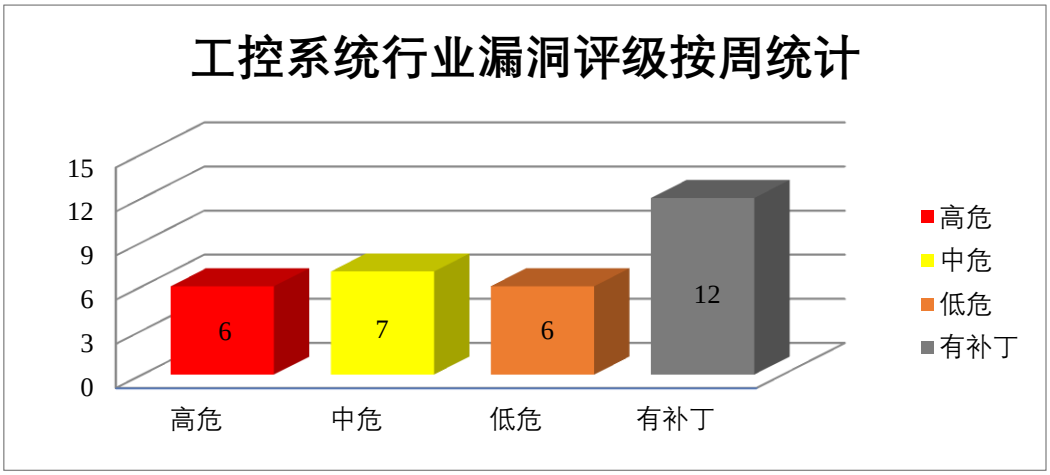

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens SINEC NMS 是德国西门子（Siemens）公司的 一个网络管理系统 (NMS)。Siemens Teamcenter Active Workspace 是一种用于访问 Teamcenter 系统的 web 应用程序。Simcenter STAR-CCM+是一个多物理计算流体动力学（CFD）软件。Siemens Teamcenter 是一套产品生命周期管理计算机软件应用程序。RUGGEDCOM RX1400 是一个多协议智能节点，将以太网交换、路由和应用程序托管功能与各种广域连接选项结合在一起。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从底层文件系统下载任意文件，获取敏感信息，绕过限制，获得 root 权限，执行代码等。

CNVD 收录的相关漏洞包括：Siemens RUGGEDCOM ROX 信息泄露漏洞、Siemens RUGGEDCOM ROX 权限提升漏洞、Siemens SINEC NMS 跨站请求伪造漏洞、Siemens SINEC NMS 路径遍历漏洞、Siemens Teamcenter Active Workspace 路径遍历漏

洞、Siemens STAR-CCM+ Viewer 越界写入漏洞、Siemens Teamcenter 访问控制错误漏洞、Siemens Teamcenter 代码问题漏洞。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-2021-71420
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71419
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71429
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71430
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71434
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71435
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71440
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71439

2、 WordPress 产品安全漏洞

WordPress 是 WordPress（Wordpress）基金会的一套使用 PHP 语言开发的博客平台。WordPress Easy Social Icons 插件是 WordPress 开源的一个应用插件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行非法 SQL 语句，获取敏感信息，窃取用户 Cookie 凭据等。

CNVD 收录的相关漏洞包括：WordPress 跨站脚本漏洞（CNVD-2021-70735）、WordPress SQL 注入漏洞（CNVD-2021-70739、CNVD-2021-70733、CNVD-2021-70738、CNVD-2021-70740）、WordPress underConstruction 跨站脚本漏洞、WordPress Gutenberg Template Library&Redux Framework 访问控制错误漏洞、WordPress Easy Social Icons 跨站脚本漏洞。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-2021-70733
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70735
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70739
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70738
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70740
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70743
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70742
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70741

3、 Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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

在执行任意代码，控制受影响的系统，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等。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 远程代码执行漏洞（CNVD-2021-71405、CNVD-2021-71406、CNVD-2021-71407、CNVD-2021-71408、CNVD-2021-71410、CNVD-2021-71411、CNVD-2021-71413、CNVD-2021-71414）。其中，“Microsoft Windows 和 Windows Server 远程代码执行漏洞（CNVD-2021-71410、CNVD-2021-71411、CNVD-2021-71413、CNVD-2021-71414）”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-2021-71405
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71406
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71407
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71408
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71410
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71411
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71413
https://www.cnvd.org.cn/flaw/show/CNVD-2021-71414

4、 IBM 产品安全漏洞

IBM Financial Transaction Manager 是美国 IBM 公司的一款金融事务管理器。IBM Planning Analytics 是一款计划、预算、预测及分析解决方案。IBM AIX 是一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM WebSphere Application Server（WAS）是由 IBM 遵照开放标准，例如 Java EE、XML 及 Web Services，开发并发行的一种应用服务器。IBM Tivoli Workload Scheduler 是一套企业任务调度软件。IBM API Connect 是一种综合的端到端 API 生命周期解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行客户端代码，获取敏感信息和根特权，注入代码等。

CNVD 收录的相关漏洞包括：IBM Financial Transaction Manager 跨站脚本漏洞（CNVD-2021-71255）、IBM Planning Analytics 信息泄露漏洞（CNVD-2021-71523、CNVD-2021-71522）、IBM AIX 权限许可和访问控制问题漏洞（CNVD-2021-71526、CNVD-2021-71529）、IBM WebSphere Application Server 权限提升漏洞（CNVD-2021-71530）、IBM Tivoli Workload Scheduler 缓冲区溢出漏洞、IBM API Connect 代码注入漏洞。其中，“IBM AIX 权限许可和访问控制问题漏洞（CNVD-2021-71526、CNVD-2021-71529）、IBM API Connect 代码注入漏洞”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-2021-71255

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71523

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71522

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71526

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71530

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71529

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71528

https://www.cnvd.org.cn/flaw/show/CNVD-2021-71527

5、Mozilla Rust 内存破坏漏洞（CNVD-2021-71659）

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，Rust may_queue crate through 2020-11-10 被披露存在命令注入漏洞。攻击者可利用该漏洞导致发生内存损坏。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-2021-71659

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-2021-70816	大华部分产品身份认证绕过漏洞	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://www.dahuasecurity.com/support/cybersecurity/details/957
CNVD-2021-71258	Aruba Networks ArubaOS 操作系统命令注入漏洞（CNVD-2021-71258）	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/tuxera/ntfs-3g
CNVD-2021-70815	大华部分产品身份认证绕过漏洞（CNVD-2021-70815）	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.dahuasecurity.com/support/cybersecurity/details/957
CNVD-2021-71257	ArubaOS 路径遍历漏洞（CNVD-2021-71257）	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-2021-71261	Aruba Networks ArubaOS 操作系统命令注入漏洞（CNVD-2021-71261）	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/tuxera/ntfs-3g
CNVD-2021-71428	Siemens SIPROTEC 5 输入验证不当漏洞	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/pdf/ssa-500748.pdf

CNVD-2021-71433	Siemens IFC adapter in NX 释放后使用漏洞	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/pdf/ssa-208530.pdf
CNVD-2021-71454	Edgegallery developer-be 代码问题漏洞	高	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://github.com/EdgeGallery/developer-be/issues/1
CNVD-2021-71441	Siemens Industrial Edge Management 授权绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-692317.pdf
CNVD-2021-71443	Siemens SIMATIC NET CP 模块拒绝服务漏洞	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/pdf/ssa-549234.pdf

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞从底层文件系统下载任意文件，获取敏感信息，绕过限制，获得 root 权限，执行代码等。此外，WordPress、Microsoft、IBM 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞执行任意代码，获取敏感信息和根特权，注入代码等。另外，Rust may_queue crate through 2020-11-10 被披露存在命令注入漏洞。攻击者可利用该漏洞导致发生内存损坏。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、TastyIgniter 跨站脚本漏洞

验证描述

TastyIgniter 是一个基于 Laravel PHP Framework 的免费开源餐厅在线订购系统。

TastyIgniter 3.0.7 存在跨站脚本漏洞，该漏洞源于软件中的/account, /reservation, /admin/dashboard，和/admin/system_logs 目录中缺少对于用户提交数据的有效验证，攻击者可利用该漏洞执行任意 JavaScript。

验证信息

POC 链接：https://packetstormsecurity.com/files/163843/TastyIgniter-3.0.7-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-71457

信息提供者

恒安嘉新(北京)科技股份公司

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. Adobe 发布 59 个漏洞补丁，涉及 Acrobat、Photoshop 等 15 种产品

Adobe 正在敦促其大批 Acrobat Reader 用户更新他们的软件，以修复可能允许攻击者在未打补丁的版本上执行任意代码的关键漏洞。

参考链接：https://www.freebuf.com/news/288689.html

2. Travis CI 漏洞影响上千万组织

Travis CI 是一家总部位于柏林的持续集成供应商，近期其修补了一个严重的漏洞，该漏洞暴露了签名密钥、API 密钥和访问凭证，使成千上万的组织面临潜在风险。

参考链接：https://www.inforisktoday.com/travis-ci-flaw-exposed-secrets-from-public-repositories-a-17535

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