国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 08 月 16 日-2021 年 08 月 22 日　　2021 年第 33 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 603 个，其中高危漏洞 166 个、中危漏洞 367 个、低危漏洞 70 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 354 个（占 59%），其中互联网上出现“WordPress 插件 Popular Posts 远程代码执行漏洞、Zoo Management System '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原创漏洞总数 12901 个，与上周（3186 个）环比增加 3.0 倍。

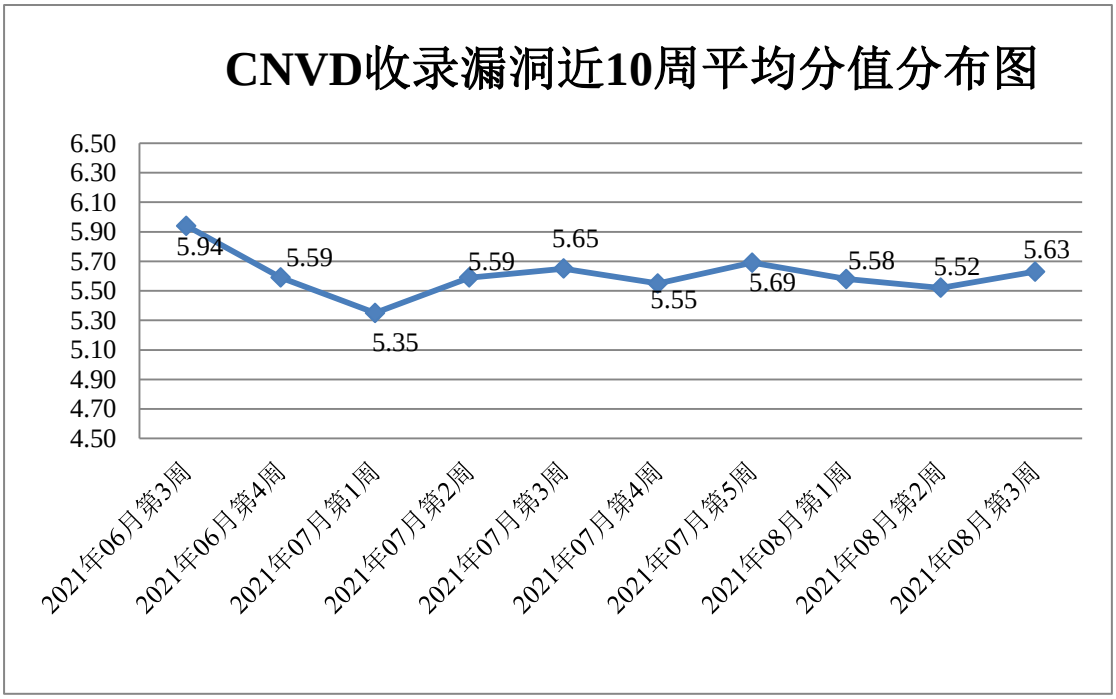

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 17 起，向基础电

信企业通报漏洞事件 42 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 461 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 49 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 53 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、珠海玖时光科技有限公司、众勤通信设备贸易（上海）有限公司、中控泰科（北京）科技发展有限公司、中航信移动科技有限公司、中国软件与技术服务股份有限公司、中国电力工程顾问集团西南电力设计院有限公司、中保无限科技有限公司、智汇方象（青岛）软件有限公司、郑州单点科技软件有限公司、郑州晨华科技有限公司、浙江核新同花顺网络信息股份有限公司、浙江杭云网络科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、优慕课在线教育科技（北京）有限责任公司、用友网络科技股份有限公司、研华科技（中国）有限公司、讯舟科技股份有限公司、新誼整合科技股份有限公司、新天科技股份有限公司、小米科技有限责任公司、先登高科电气有限公司、西安紫云羚网络科技有限责任公司、微软（中国）有限公司、泰安梦泰尔软件有限公司、苏州科达科技股份有限公司、四三九九网络股份有限公司、四创科技有限公司、石家庄市征红网络科技有限公司、神彩科技股份有限公司、深圳市易佰网络科技有限公司、深圳市微控一指通科技有限公司、深圳市科迈爱康科技有限公司、深圳市吉祥腾达科技有限公司、深圳市德传技术有限公司、深圳市必联电子有限公司、深圳警翼智能科技股份有限公司、上海纵之格科技有限公司、上海商创网络科技有限公司、上海桑锐电子科技股份有限公司、上海绮梦网络科技有限公司、上海华测导航技术股份有限公司、上海格尔软件股份有限公司、上海泛微网络科技股份有限公司、上海二三四五移动科技有限公司、上海得淼科技发展有限公司、山石网科通信技术（北京）有限公司、山东金钟科技集团股份有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、青岛易企天创管理咨询有限公司、普联技术有限公司、鹏为软件股份有限公司、南宁火蝶科技有限公司、南京广真信息科技有限公司、纳里健康科技有限公司、洛阳尚贤网络科技有限公司、零视技术（上海）有限公司、理光（中国）投资有限公司、江西金磊科技发展有限公司、江苏倢科软件有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、华数传媒网络有限公司、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、洪湖尔创网联信息技术有限公司、杭州海康威视系统技术有限公司、杭州冠航科技有限公司、汉王科技股份有限公司、海南旗鱼科技有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、广州市联展贸易有限公司、广州市保伦电子有限公司、广州南方卫星导航仪器有限公司、广州鼎成信息科技有限公司、广联达科技股份有限公司、广东卓锐软件有限公司、

广东凯格科技有限公司、福建银达汇智信息科技股份有限公司、钉钉（中国）信息技术有限公司、大唐电信科技股份有限公司、大明重工有限公司、大连理工计算机控制工程有限公司、驰宇科技有限公司、成都零起飞科技有限公司、成都光大网络科技有限公司、成都爱米秀科技有限责任公司、博世（中国）投资有限公司、北京中庆纳博信息技术有限公司、北京中科新远科技有限公司、北京中创视讯科技有限公司、北京中成科信科技发展有限公司、北京哲博科技有限公司、北京因酷时代科技有限公司、北京亚鸿世纪科技发展有限公司、北京星网锐捷网络技术有限公司、北京微鲤科技有限公司、北京威速科技有限公司、北京搜狗信息服务有限公司、北京时空智友科技有限公司、北京蚂蜂窝网络科技有限公司、北京金和网络股份有限公司、北京火木科技有限公司、北京汉邦高科数字技术股份有限公司、北京畅聊天下科技股份有限公司、暴风集团股份有限公司、安徽品格网络科技有限公司、爱普生（中国）有限公司、猎豹移动、腾讯安全应急响应中心、帝国软件、智睿软件、爱青檬 CMS、梦想 CMS、熊海 CMS、若依、ZZCMS、zcncms、YZNCMS、waychar、VMware、UGRID、ThinkAdmin、The Apache Software Foundation、SemCms、SchoolCMS、PHPMyWind、NETGEAR、MuYuCMS、MacCMS、Dreamer CMS、dcrcms、Broadcom、AppCMS、AKCMS 和 365cam。

本周，CNVD 发布了《Microsoft 发布 2021 年 8 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6751

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、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、北京数字观星科技有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、南京联成科技发展股份有限公司、内蒙古奥创科技有限公司、北京长亭科技有限公司、卫士通信息产业股份有限公司、西安四叶草信息技术有限公司、北京智游网安科技有限公司、联想全球安全实验室、北京华云安信息技术有限公司、中国电信股份有限公司网络安全产品运营中心、河南灵创电子科技有限公司、内蒙古云科数据服务股份有限公司、北京山石网科信息技术有限公司、山东云天安全技术有限公司、阿里巴巴网络技术有限公司、浙江木链物联网科技有限公司、北京天地和兴科技有限公司、广东蓝爵网络安全技术股份有限公司、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、南京众智维信息科技有限公司、山东泽鹿安全技术有限公司、浙江大华技术股份有限公司、安徽长泰信息安全服务有限公司、信联科技（南京）有限公司、京东云安全、长春嘉诚信息技术股份有限公司、重庆都会信息科技有限公司、北京远禾科技有限公司、河南金盾信安检测评估中心、泰山信息科技有限公司、

山东新潮信息技术有限公司、上海纽盾科技股份有限公司、物鼎安全科技（武汉）有限公司、北京惠而特科技有限公司、中安网盾（广州）信息科技有限公司、四川哨兵信息科技有限公司、亚信科技（成都）有限公司、南京树安信息技术有限公司、山石网科通信技术股份有限公司、浙江乾冠信息安全研究院、海南神州希望网路有限公司、星云博创科技有限公司、杭州迪普科技股份有限公司、北方实验室（沈阳）股份有限公司、浙江国利网安科技有限公司、四川赛虎科技有限公司（玄蜂安全团队）、深圳市魔方安全科技有限公司、武汉明嘉信信息安全检测评估有限公司、中金金融认证中心有限公司、河南天祺信息安全技术有限公司、北京信联科汇科技有限公司、广州安亿信软件科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）及其他个人白帽子向 CNVD 提交了 12901 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 10292 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
奇安信网神（补天平台）	8880	8880
斗象科技（漏洞盒子）	1029	1029
北京神州绿盟科技有限公司	506	4
上海交大	383	383
北京天融信网络安全技术有限公司	300	2
哈尔滨安天科技集团股份有限公司	274	0
北京数字观星科技有限公司	247	0
远江盛邦（北京）网络安全科技股份有限公司	240	240
北京启明星辰信息安全技术有限公司	216	162
华为技术有限公司	131	0
恒安嘉新（北京）科技股份公司	125	0
新华三技术有限公司	90	0
深信服科技股份有限公司	79	0
北京奇虎科技有限公司	67	10
天津市国瑞数码安全系统股份有限公司	59	0

（国瑞数码零点实验室）		
南京联成科技发展股份有限公司	12	12
内蒙古奥创科技有限公司	10	10
北京长亭科技有限公司	6	6
卫士通信息产业股份有限公司	6	6
北京知道创宇信息技术股份有限公司	6	0
西安四叶草信息技术有限公司	4	4
北京智游网安科技有限公司	1	1
北京山石网科信息技术有限公司	414	414
联想全球安全实验室	168	1
山东云天安全技术有限公司	163	163
北京华云安信息技术有限公司	151	151
中国电信股份有限公司网络安全产品运营中心	119	77
河南灵创电子科技有限公司	46	46
内蒙古云科数据服务股份有限公司	45	45
浙江木链物联网科技有限公司	36	36
广东蓝爵网络安全技术股份有限公司	31	31
阿里巴巴网络技术有限公司	30	30
北京天地和兴科技有限公司	29	29
杭州海康威视数字技术股份有限公司	26	26
北京安帝科技有限公司	24	24
南京众智维信息科技	16	16

有限公司		
山东泽鹿安全技术有限公司	16	16
上海纽盾科技股份有限公司	15	15
北京信联科汇科技有限公司	15	15
浙江大华技术股份有限公司	13	13
安徽长泰信息安全服务有限公司	13	13
信联科技（南京）有限公司	12	12
山东新潮信息技术有限公司	12	12
京东云安全	11	11
北京云科安信科技有限公司（Seraph 安全实验室）	11	11
长春嘉诚信息技术股份有限公司	10	10
重庆都会信息科技有限公司	9	9
北京远禾科技有限公司	8	8
泰山信息科技有限公司	7	7
河南金盾信安检测评估中心	6	6
北京惠而特科技有限公司	5	5
物鼎安全科技（武汉）有限公司	4	4
中安网盾（广州）信息科技有限公司	3	3
四川哨兵信息科技有限公司	3	3
亚信科技（成都）有限公司	2	2
南京树安信息技术有限公司	2	2
山石网科通信技术股份有限公司	2	2

浙江乾冠信息安全研究院	2	2
星云博创科技有限公司	2	2
海南神州希望网路有限公司	1	1
杭州迪普科技股份有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
浙江国利网安科技有限公司	1	1
四川赛虎科技有限公司（玄蜂安全团队）	1	1
深圳市魔方安全科技有限公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
中金金融认证中心有限公司	1	1
河南天祺信息安全技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
西门子（中国）有限公司	1	0
CNCERT 宁夏分中心	4	4
CNCERT 西藏分中心	2	2
CNCERT 山西分中心	1	1
个人	863	863
报送总计	15033	12901

本周漏洞按类型和厂商统计

本周，CNVD 收录了 603 个漏洞。WEB 应用 215 个，应用程序 189 个，操作系统 89 个，网络设备（交换机、路由器等网络端设备）78 个，智能设备（物联网终端设备）19 个，安全产品 13 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	215
应用程序	189
操作系统	89

网络设备（交换机、路由器等网络端设备）	78
智能设备（物联网终端设备）	19
安全产品	13

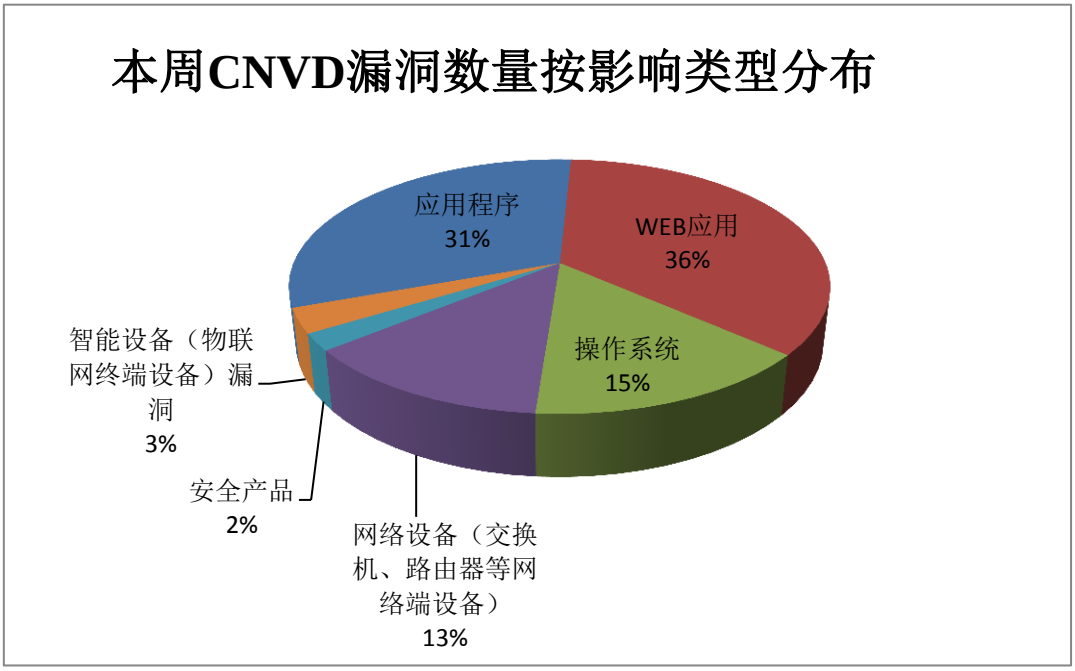

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、HuCart 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	Microsoft	73	12%
2	Google	51	8%
3	HuCart	33	6%
4	Adobe	32	6%
5	fbx-conv	26	4%
6	NETGEAR	25	4%
7	Liferay	20	3%
8	超级外卖 Super Cms	15	2%
9	Schneider Electric	11	2%
10	其他	317	53%

本周行业漏洞收录情况

本周，CNVD 收录了 51 个电信行业漏洞，23 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Nexus Control Panel 缓冲区溢出漏洞（CNVD-2021-62179）、MAC1100 PLC 拒绝服务漏洞、Google Android wifi driver 信息泄露漏洞”等漏

洞的综合评级为“高危”。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/

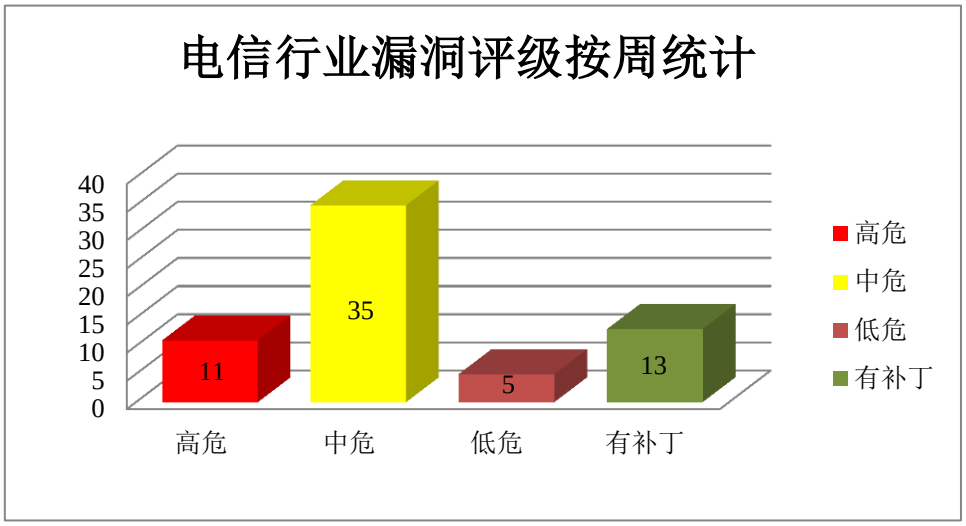

图 3 电信行业漏洞统计

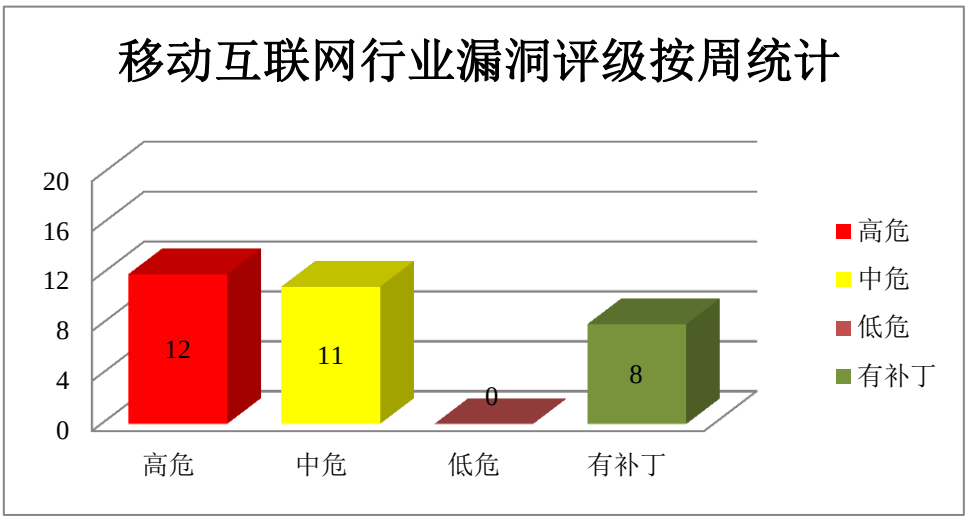

图 4 移动互联网行业漏洞统计

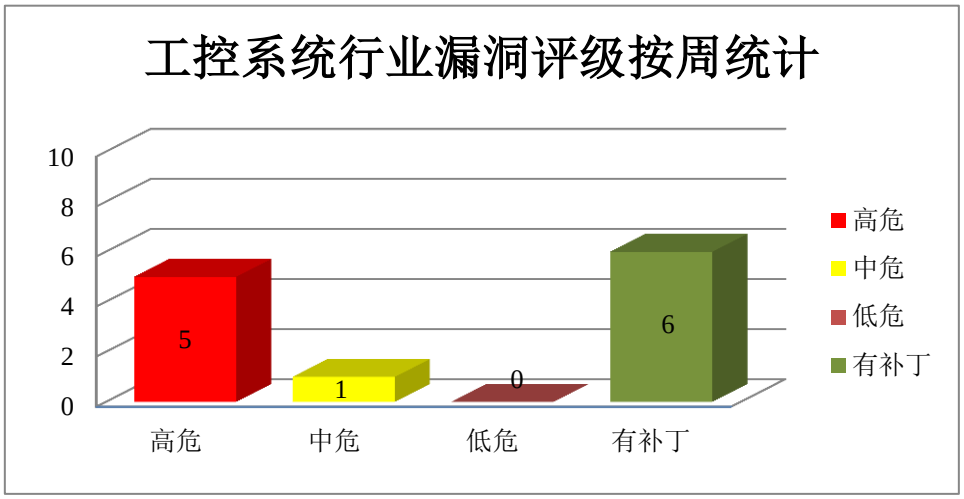

图 5 工控系统行业漏洞统计

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 TensorFlow 是一个端到端开源机器学习平台。Chrome 是由 Google 开发的一款 Web 浏览工具。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，执行任意代码或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome 越界读取漏洞（CNVD-2021-62186）、Google Chrome 释放后重用漏洞（CNVD-2021-62185、CNVD-2021-62188）、Google Chrome 堆缓冲区溢出漏洞（CNVD-2021-62189）、Google TensorFlow input_splits tensor 代码执行漏洞、Google TensorFlow tf.raw_ops.BoostedTreesCreateEnsemble 代码执行洞、Google TensorFlow MKL 代码执行漏洞、Google TensorFlow 任意代码执行漏洞。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-2021-62186

https://www.cnvd.org.cn/flaw/show/CNVD-2021-62185

https://www.cnvd.org.cn/flaw/show/CNVD-2021-62189

https://www.cnvd.org.cn/flaw/show/CNVD-2021-62188

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63061

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63068

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63072

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63084

2、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远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows/Windows Server 远程代码执行漏洞（CNVD-2021-62473、CNVD-2021-62472、CNVD-2021-62479、CNVD-2021-62484、CNVD-2021-62483、CNVD-2021-62487、CNVD-2021-62490、CNVD-2021-62489）。其中，除“Microsoft Windows/Windows Server 远程代码执行漏洞（CNVD-2021-62484、CNVD-2021-62483）”外，其余漏洞的综合评级为“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-2021-62473
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62472
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62479
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62484
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62483
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62487
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62490
https://www.cnvd.org.cn/flaw/show/CNVD-2021-62489

3、Adobe 产品安全漏洞

Adobe XMP Toolkit SDK 是美国奥多比（Adobe）公司的一种标签技术，允许您将有关文件的数据（称为元数据）嵌入到文件本身中。Adobe Bridge 是 Adobe 公司推出的一款免费数字资产管理应用程序。Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Adobe XMP Toolkit SDK 堆缓冲区溢出漏洞（CNVD-2021-63256、CNVD-2021-63260、CNVD-2021-63259）、Adobe Bridge 越界读取漏洞（CNVD-2021-63274）、Adobe Photoshop 堆缓冲区溢出漏洞（CNVD-2021-63278）、Adobe Photoshop 越界写入漏洞（CNVD-2021-63277）、Adobe Bridge 越界写入漏洞（CNVD-2021-63281）、Adobe Bridge 堆缓冲区溢出漏洞（CNVD-2021-63280）。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-2021-63256
https://www.cnvd.org.cn/flaw/show/CNVD-2021-63260
https://www.cnvd.org.cn/flaw/show/CNVD-2021-63259
https://www.cnvd.org.cn/flaw/show/CNVD-2021-63274
https://www.cnvd.org.cn/flaw/show/CNVD-2021-63278

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63277

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63281

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63280

4、NETGEAR 产品安全漏洞

NETGEAR M4300-28G、NETGEAR R6400、NETGEAR R6700、NETGEAR D6100、NETGEAR EX7000、NETGEAR D6220、NETGEAR R6300、NETGEAR EX3700、NETGEAR DGN2200、NETGEAR R8900 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，攻击者可利用漏洞提升权限，执行非法命令，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品权限提升漏洞（CNVD-2021-63373）、多款 NETGEAR 产品命令注入漏洞（CNVD-2021-63372、CNVD-2021-63379）、NETGEAR 权限提升漏洞、NETGEAR 缓冲区溢出漏洞（CNVD-2021-63378、CNVD-2021-63380）、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-63381、CNVD-2021-63773）。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-2021-63373

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63372

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63375

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63378

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63381

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63380

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63379

https://www.cnvd.org.cn/flaw/show/CNVD-2021-63773

5、Portlandlabs Concrete5 代码问题漏洞

Portlandlabs Concrete5 是美国 PortlandLabs（Portlandlabs）公司的一套开源内容管理系统（CMS）。本周，Portlandlabs concrete5 被披露存在代码问题漏洞。攻击者可利用该漏洞将专门设计的数据传递给应用程序，并在目标系统上执行任意 PHP 代码。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-2021-62465

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-2021-62168	Google Chrome 栈缓冲区溢出漏洞（CNVD-2021-62168）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html
CNVD-2021-62178	Nexus Control Panel 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://us-cert.cisa.gov/ics/advisories/icsma-21-215-01
CNVD-2021-62466	Taiwan Secom Personnel Attendance Management 信任管理问题漏洞	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.chtsecurity.com/
CNVD-2021-63279	Adobe Bridge 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://helpx.adobe.com/security/products/bridge/apsb21-69.html
CNVD-2021-63768	Dell Wyse ThinOS 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.dell.com/support/kbdoc/000189543
CNVD-2021-63765	Shopware 命令注入漏洞	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/shopware/platform/security/advisories/GHSA-xh55-2fqp-p775
CNVD-2021-63774	SIEMENS SINEMA Remote Connect Server 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://cert-portal.siemens.com/productcert/pdf/ssa-816035.pdf
CNVD-2021-62182	Nexus Control Panel 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://us-cert.cisa.gov/ics/advisories/icsma-21-215-01
CNVD-2021-63766	Shopware 代码问题漏洞（CNVD-2021-63766）	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/shopware/platform/security/advisories/GHSA-gcvv-gq92-x94r
CNVD-2021-62181	Nexus Control Panel 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://us-cert.cisa.gov/ics/advisories/icsma-21-215-01

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，执行任意代码或导致应用程序崩溃。此外，Microsoft、Adobe、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务等。

另外，Portlandlabs Concrete5 被披露存在代码问题漏洞。攻击者可利用该漏洞将专门设计的数据传递给应用程序，并在目标系统上执行任意 PHP 代码。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 插件 Popular Posts 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 插件 Popular Posts 存在远程代码执行漏洞，攻击者可以利用该漏洞远程执行任意代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/50129

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-63785

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. Realtek Wi-Fi SDK 的多个漏洞影响近百万物联网设备

台湾芯片设计商 Realtek 警告其 WiFi 模块附带的三个软件开发工具包（SDK）中存在四个安全漏洞，这些软件开发工具包用于至少 65 家供应商生产的近 200 款物联网设备。

参考链接：https://thehackernews.com/2021/08/multiple-flaws-affecting-realtek-wi-fi.html

2. 美国官方曝光网络摄像头大漏洞，超 8300 万台设备受影响

美国联邦网络安全和基础设施安全局公布了一个影响数以千万计的物联网设备的严重漏洞，攻击者不仅能够通过该漏洞看到安全网络摄像头等设备拍摄的实时视频，还能利用该漏洞控制这些设备。

参考链接：https://finance.sina.com.cn/tech/2021-08-19/doc-ikqcfncc3776753.shtml

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