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 09 日-2021 年 08 月 15 日　　2021 年第 32 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 135 个、中危漏洞 403 个、低危漏洞 65 个。漏洞平均分值为 5.52。本周收录的漏洞中，涉及 0day 漏洞 382 个（占 63%），其中互联网上出现“Accela Civic Platform 信息泄露漏洞、GetSimple CMS 跨站脚本漏洞（CNVD-2021-61755）”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 3186 个，与上周（3796 个）环比减少 16%。

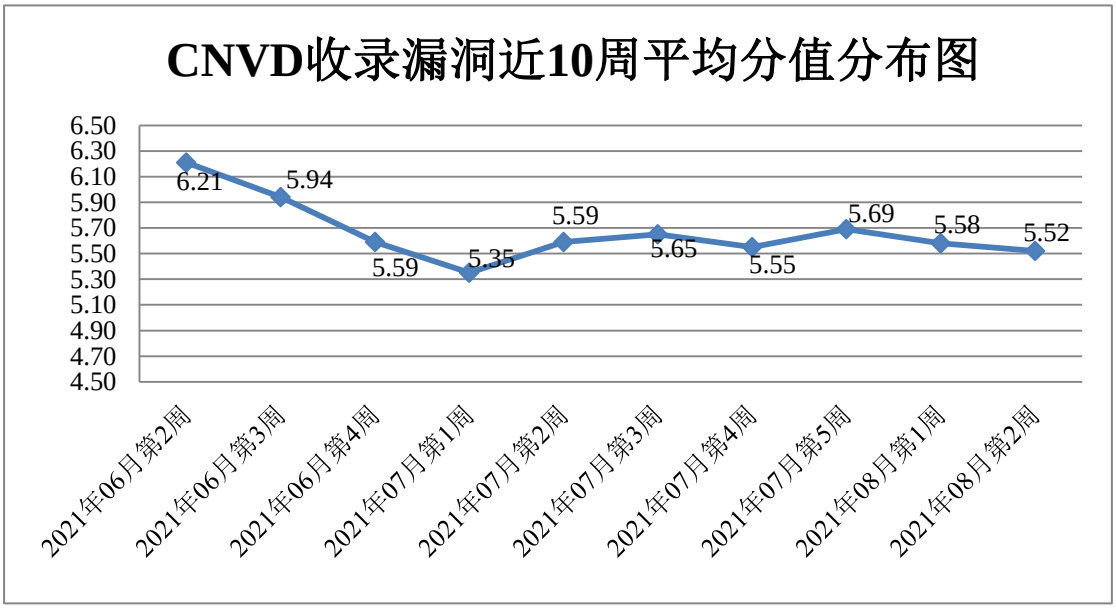

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 39 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 351 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 57 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 26 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、众勤通信设备贸易（上海）有限公司、中国电信集团有限公司、郑州慧森信息有限责任公司、镇江市云优网络科技有限公司、浙江深大智能科技有限公司、浙江齐治科技股份有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、新锐亚科技（北京）有限公司、新岸线（北京）科技集团有限公司、小鱼视讯（北京）科技有限公司、西安交大捷普网络科技有限公司、武汉思为同飞网络技术股份有限公司、武汉神州数码云科网络技术有限公司、无锡城安信息科技有限公司、卫宁健康科技集团股份有限公司、伟乐视讯科技股份有限公司、微软（中国）有限公司、网际傲游（北京）科技有限公司、同程网络科技股份有限公司、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、四川迅睿云软件开发有限公司、烁博信息科技（上海）有限公司、世邦通信股份有限公司、神彩科技股份有限公司、深圳维盟科技股份有限公司、深圳市中科新业信息科技发展有限公司、深圳市中科网威科技有限公司、深圳市智开科技有限公司、深圳市圆梦云科技有限公司、深圳市友华通信技术有限公司、深圳市鑫塔科技有限公司、深圳市网域科技技术有限公司、深圳市万普拉斯科技有限公司、深圳市仕方通信科技有限公司、深圳市龙信信息技术有限公司、深圳市联天通信技术有限公司、深圳市利谱信息技术有限公司、深圳市锟铻科技有限公司、深圳市甲易科技有限公司、深圳市吉祥腾达科技有限公司、深圳市华博科技开发有限公司、深圳市广道高新技术股份有限公司、深圳市福洽科技有限公司、深圳市发掘科技有限公司、深圳市大洲智创科技有限公司、深圳市朝恒辉网络科技有限公司、深圳市安盟信息科技有限公司、深圳齐杉科技有限公司、深圳华域数安科技有限公司、深圳国视安科技有限公司、深圳国人通信股份有限公司、深圳奥联信息安全技术有限公司、上海纵之格科技有限公司、上海卓佑计算机技术有限公司、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、上海商派网络科技有限公司、上海纽盾科技股份有限公司、上海华依科技集团股份有限公司、上海华测导航技术股份有限公司、上海布谷网络科技有限公司、上海冰峰网络科技有限公司、上海爱数信息技术股份有限公司、上海艾泰网络信息有限公司、山东潍微科技股份有限公司、山东仁科测控技术有限公司、山东金钟科技集团股份有限公司、厦门才茂通信科技有限公司、全球系统股份整合有限公司、青岛通软网络科技有限公司、普联技术有限公司、南宁市安拓软件有限公司、南京维盟网络科技有限公司、迈普通信技术股份有限公司、辽宁微时光科技有限公司、乐视网信息技术（北京）股份有限公司、科大讯飞股份有限公司、今信天

安（北京）科技有限公司、江苏汇文软件有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、华信数安（深圳）技术有限公司、华硕电脑（上海）有限公司、湖南中彩科技有限公司、湖南奥科网络技术股份有限公司、湖北力达科讯科技发展有限公司、河南安冉云网络科技有限公司、合信致远信息技术（北京）有限公司、合肥明信软件技术有限公司、杭州盈高科技有限公司、杭州叙简科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州临企网络技术有限公司、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、广州智臣信息科技有限公司、广州网易计算机系统有限公司、广州同聚成电子科技有限公司、广州市奥威亚电子科技有限公司、广州热点软件科技股份有限公司、广州齐博网络科技有限公司、广州巨泰电子科技有限公司、广州红帆科技有限公司、广州国微软件科技有限公司、广州丰川网络科技有限公司、广州鼎成信息科技有限公司、广东广晟通信技术有限公司、富士施乐（中国）有限公司、福建中信网安信息科技有限公司、福建省海峡信息技术有限公司、福建福昕软件开发股份有限公司、飞思达技术（北京）有限公司、大唐电信科技股份有限公司、大连华天软件有限公司、北京卓越信通电子股份有限公司、北京逐风科技有限公司、北京中科网威信息技术有限公司、北京长亭未来科技有限公司、北京熊宝贝科技发展有限公司、北京星网锐捷网络技术有限公司、北京信达网安信息技术有限公司、北京信安世纪科技股份有限公司、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、北京网际思安科技有限公司、北京万维盈创科技发展有限公司、北京天信瑞安科技股份有限公司、北京世纪网展科技有限公司、北京圣博润高新技术股份有限公司、北京声智科技有限公司、北京神州数码云科信息技术有限公司、北京瑞星网安技术股份有限公司、北京趋势恒信科技有限公司、北京朗新天霁软件技术有限公司、北京科信欧亿科技有限公司、北京开维创科技有限公司、北京金和网络股份有限公司、北京火木科技有限公司、北京华清信安科技有限公司、北京合信同达科技有限公司、北京国炬信息技术有限公司、北京格尔国信科技有限公司、北京飞书科技有限公司、北京北信源软件股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、凹盾（北京）科技有限公司、安科讯（福建）科技有限公司、安徽阳光心健心理咨询有限公司、爱普生（中国）有限公司、网展科技、智睿软件、若依、阿里巴巴集团安全应急响应中心、梦想 CMS、MyfCMS-闵益飞内容管理系统、SAHO 商合行、zzcms、ZAVIO、WordPress、waychar、Sumatra PDF、Nitro、NETGEAR、Kyan、HuCart、BigAntSoft、AppCMS、Amazon Web Services, Inc.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、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京数字观星科技有限公司、恒安嘉新（北京）科技股份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、

北京山石网科信息技术有限公司、北京信联科汇科技有限公司、浙江木链物联网科技有限公司、北京华云安信息技术有限公司、山东泽鹿安全技术有限公司、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、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、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、山东新潮信息技术有限公司、重庆都会信息科技有限公司、北京惠而特科技有限公司、安徽长泰信息安全服务有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海纽盾科技股份有限公司、江苏快页信息技术有限公司、星云博创科技有限公司、武汉明嘉信信息安全检测评估有限公司、南京树安信息技术有限公司、百度在线网络技术有限公司、北京边界无限科技有限公司、福建中信网安信息科技有限公司、中安网盾（广州）信息科技有限公司、浙江大学控制科学与工程学院、中通服咨询设计研究院有限公司、浙江乾冠信息安全研究院、四川赛虎科技有限公司、北京远禾科技有限公司、浙江国利网安科技有限公司、小安（北京）科技有限公司、深圳市魔方安全科技有限公司、上海市信息安全测评认证中心、上海嘉韦思信息技术有限公司、河南信安世纪科技有限公司、杭州美创科技有限公司、杭州迪普科技股份有限公司、广州乐轩玄彩电子科技有限公司、东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室、北京云弈科技有限公司、北京君云天下科技有限公司及其他个人白帽子向 CNVD 提交了 3186 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）、和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 683 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
北京天融信网络安全技术有限公司	562	50
斗象科技（漏洞盒子）	354	354
奇安信网神（补天平台）	329	329
哈尔滨安天科技集团股份有限公司	270	0
华为技术有限公司	129	0
北京数字观星科技有限公司	128	0

恒安嘉新（北京）科技股份公司	126	0
新华三技术有限公司	119	0
北京启明星辰信息安全技术有限公司	116	56
北京神州绿盟科技有限公司	101	8
深信服科技股份有限公司	89	4
国瑞数码零点实验室	59	0
内蒙古奥创科技有限公司	36	36
北京奇虎科技有限公司	18	18
南京联成科技发展股份有限公司	15	15
浙江大华技术股份有限公司	9	9
北京知道创宇信息技术股份有限公司	5	0
北京安信天行科技有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	1	1
山东云天安全技术有限公司	243	243
北京山石网科信息技术有限公司	183	183
北京信联科汇科技有	181	181

限公司		
浙江木链物联网科技有限公司	125	125
北京华云安信息技术有限公司	111	111
联想集团	103	0
山东泽鹿安全技术有限公司	75	75
西门子（中国）有限公司	59	0
河南灵创电子科技有限公司	41	41
南京众智维信息科技有限公司	37	37
广东蓝爵网络安全技术股份有限公司	27	27
北京天地和兴科技有限公司	23	23
杭州海康威视数字技术股份有限公司	18	18
北京安帝科技有限公司	16	16
山东新潮信息技术有限公司	14	14
重庆都会信息科技有限公司	13	13
北京惠而特科技有限公司	12	12
安徽长泰信息安全服务有限公司	12	12
北京云科安信科技有限公司（Seraph 安全	11	11

实验室）		
上海纽盾科技股份有限公司	9	9
江苏快页信息技术有限公司	9	9
星云博创科技有限公司	7	7
武汉明嘉信信息安全检测评估有限公司	6	6
南京树安信息技术有限公司	6	6
百度在线网络技术有限公司	5	5
北京边界无限科技有限公司	4	4
福建中信网安信息科技有限公司	3	3
中安网盾（广州）信息科技有限公司	3	3
浙江大学控制科学与工程学院	3	3
中通服咨询设计研究院有限公司	2	2
浙江乾冠信息安全研究院	2	2
四川赛虎科技有限公司	2	2
北京远禾科技有限公司	2	2
浙江国利网安科技有限公司	1	1
小安（北京）科技有限公司	1	1
深圳市魔方安全科技	1	1

有限公司		
上海市信息安全测评认证中心	1	1
上海嘉韦思信息技术有限公司	1	1
河南信安世纪科技有限公司	1	1
杭州美创科技有限公司	1	1
杭州迪普科技股份有限公司	1	1
广州乐轩玄彩电子科技有限公司	1	1
东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室	1	1
北京云弈科技有限公司	1	1
北京君云天下科技有限公司	1	1
CNCERT 贵州分中心	4	4
CNCERT 青海分中心	4	4
CNCERT 西藏分中心	2	2
CNCERT 山东分中心	2	2
个人	1074	1074
报送总计	4934	3186

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 268 个，应用程序 142 个，网络设备（交换机、路由器等网络端设备）80 个，操作系统 58 个，智能设备（物联网终端设备）34 个，安全产品 21 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	268
应用程序	142
网络设备（交换机、路由器等网络端设备）	80
操作系统	58
智能设备（物联网终端设备）漏洞	34
安全产品	21

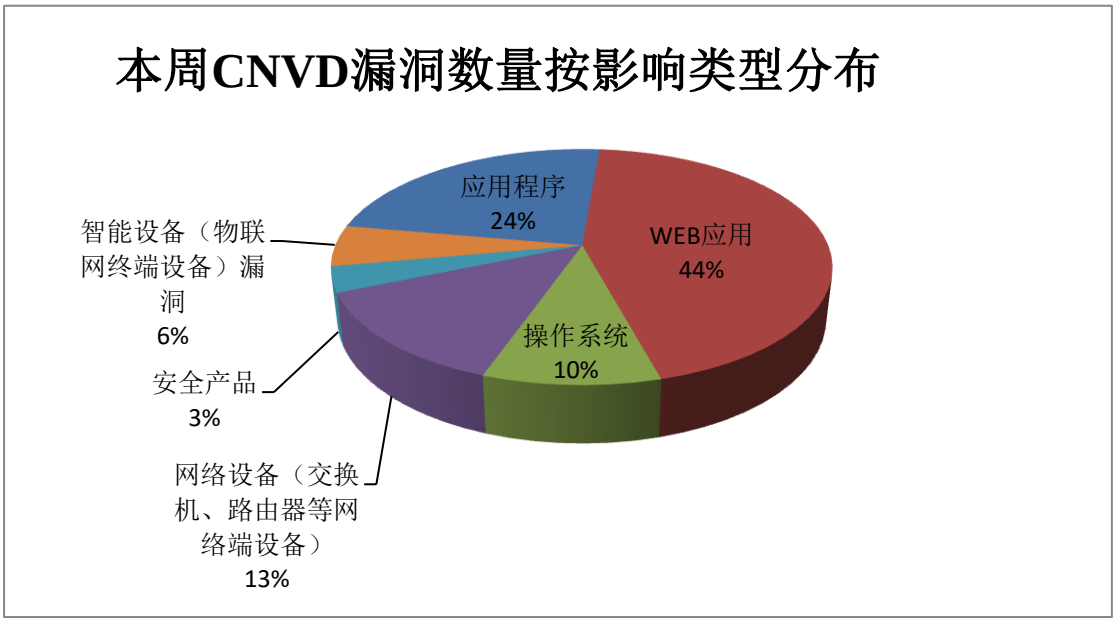

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、武汉爱码农网络科技有限公司、WordPress 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	33	6%
2	武汉爱码农网络科技有限公司	31	5%
3	WordPress	25	4%
4	Cybozu	24	4%
5	NETGEAR	24	4%
6	Linux	17	3%
7	Santesoft	16	3%
8	Mozilla	15	2%
9	CourseSEL	12	2%
10	其他	406	67%

本周行业漏洞收录情况

本周，CNVD 收录了 53 个电信行业漏洞，13 个移动互联网行业漏洞，13 个工控行

业漏洞（如下图所示）。其中，“Siemens Automation License Manager 拒绝服务漏洞（CNVD-2021-61126）、IBM Content Navigator 拒绝服务漏洞、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-61052）”等漏洞的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/

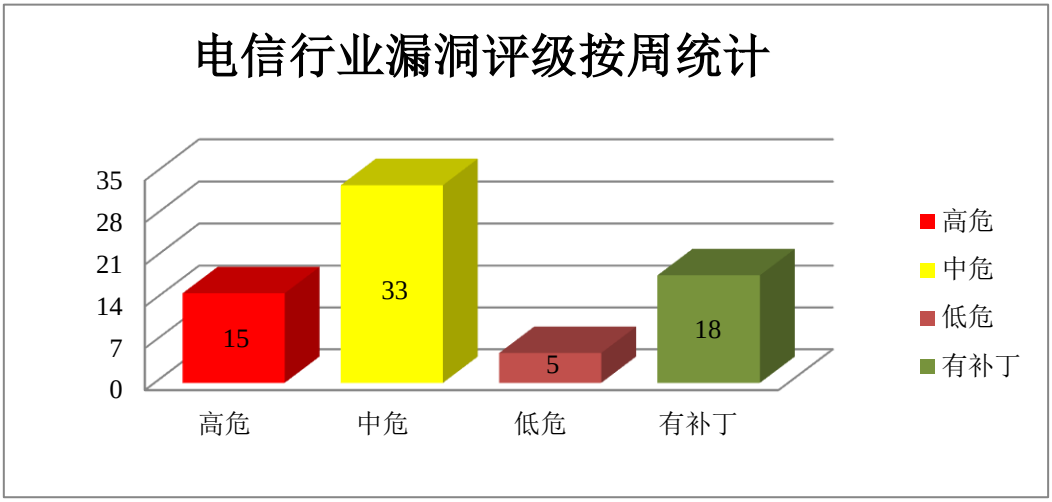

图 3 电信行业漏洞统计

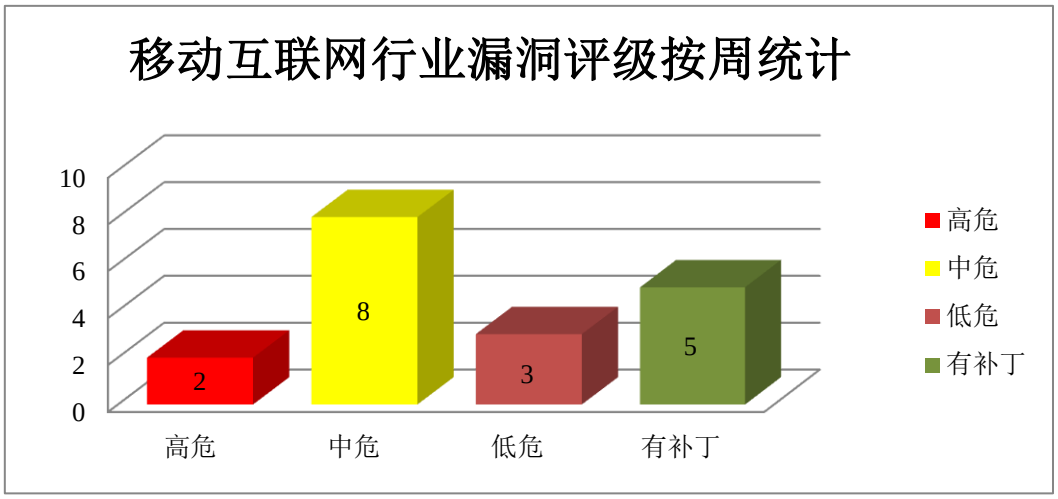

图 4 移动互联网行业漏洞统计

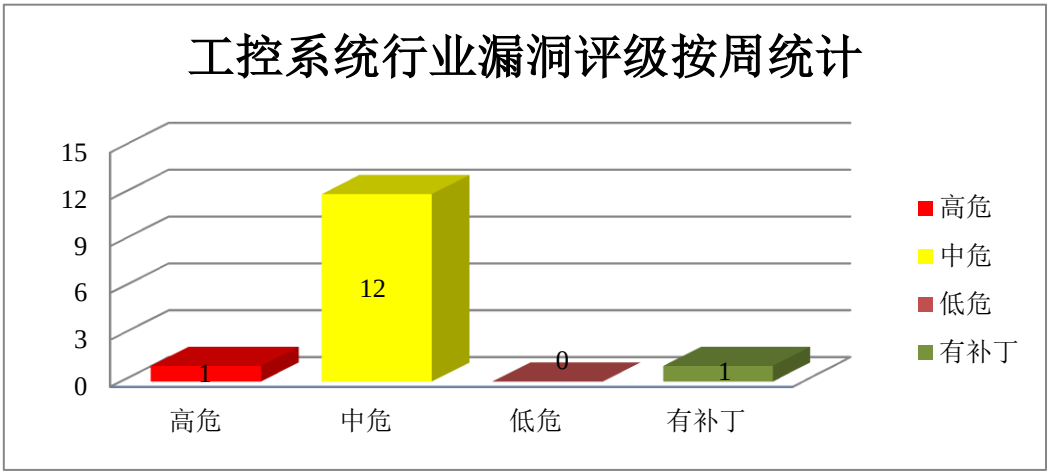

图 5 工控系统行业漏洞统计

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、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。Microsoft Visual Studio Code 是一款开源的代码编辑器。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，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Visual Studio Code 命令注入漏洞（CNVD-2021-61415）、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-61773、CNVD-2021-61772、CNVD-2021-61771、CNVD-2021-61777、CNVD-2021-61781、CNVD-2021-61784、CNVD-2021-61782）。其中，除“Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-61772、CNVD-2021-61771、CNVD-2021-61777）”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-2021-61415

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61773

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61772

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61771

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61777

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61781

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61784

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61782

2、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 SIMATIC S7-1200 是一款 S7-1200 系列 PLC（可编程逻辑控制器）。SIMATIC S7-1500 CPU 是一款 CPU（中央处理器）模块。SIMATIC S7-1500 是一款可编程逻辑控制器。Siemens Solid Edge 是一款三维 CAD 软件。Siemens Automation License Manager 集中管理各种西门子软件产品的许可证密钥。Siemens Jt2go 是一款 JT 文件查看器。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。本周，上述产品被披露存在未授权访问漏洞，攻击者可利用漏洞绕过身份验证，越界访问，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens Jt2go 和 Teamcenter Visualization 空指针解引用漏洞、Siemens SINEC NMS OS 命令注入漏洞、Siemens SIMATIC S7-1200 缺少身份验证漏洞、Siemens SIMATIC S7-1500 CPU 和 SIMATIC S7-1500 不正确授权漏洞、Siemens Solid Edge XML 外部实体注入漏洞、Siemens Solid Edge 释放后重用漏洞、Siemens Solid Edge 缓冲区溢出漏洞（CNVD-2021-61127）、Siemens Automation License Manager 拒绝服务漏洞（CNVD-2021-61126）。其中“Siemens SINEC NMS OS 命令注入漏洞、Siemens SIMATIC S7-1200 缺少身份验证漏洞、Siemens Solid Edge 释放后重用漏洞、Siemens Solid Edge 缓冲区溢出漏洞（CNVD-2021-61127）”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-2021-61125
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61124
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61123
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61122
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61129
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61128
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61127
https://www.cnvd.org.cn/flaw/show/CNVD-2021-61126

3、NETGEAR 产品安全漏洞

NETGEAR D8500、NETGEAR R7800、NETGEAR D6100、NETGEAR WNDR3700、NETGEAR R8900、NETGEAR EX7000、NETGEAR R6250 都是美国网件（NETGEAR）公司的无线路由器产品。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 产品命令注入漏洞（CNVD-2021-61058、CNVD-2021-61057）、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-61056、CNVD-2021-61059、CNVD-2021-61062、CNVD-2021-61061、CNVD-2021-61060、CNVD-2021-61054）。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-2021-61054

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61058

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61057

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61056

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61059

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61062

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61061

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61060

4、WordPress 产品安全漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入任意的 web 脚本或 HTML，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：WordPress 跨站请求伪造漏洞（CNVD-2021-59587）、WordPress W3 Total Cache 插件跨站脚本漏洞、WordPress WP Image Zoom 插件文件包含漏洞、WordPress Event Espresso Core 跨站脚本漏洞、WordPress 插件跨站脚本漏洞（CNVD-2021-59594、CNVD-2021-59603）、WordPress 信息泄露漏洞（CNVD-2021-59604）、WordPress SQL 注入漏洞（CNVD-2021-61432）。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-2021-59587

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59589

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59588

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59591

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59594

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59603

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59604

https://www.cnvd.org.cn/flaw/show/CNVD-2021-61432

5、Advantech WebAccess HMI Designer 缓冲区溢出漏洞（CNVD-2021-60558）

Advantech WebAccess HMI Designer 是中国台湾研华（Advantech）公司的一款人机界面集成开发工具。本周，Advantech WebAccess HMI Designer 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞使用专门设计的项目文件，触发基于堆的缓冲区溢出，并在目标系统上执行任意代码。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-2021-60558

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-2021-59764	Cisco Small Business RV160 和 RV260 系列 VPN 路由器远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4
CNVD-2021-60510	Huawei HarmonyOS 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077
CNVD-2021-60517	Linux kernel 拒绝服务漏洞（CNVD-2021-60517）	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://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4
CNVD-2021-60532	Fortinet FortiPortal 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://www.cybersecurity-help.cz/vdb/SB2021080312
CNVD-2021-60539	Zoho ManageEngine ADManager Plus 远程代码执行漏洞	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.manageengine.com/
CNVD-2021-60550	Zscaler Client Connector 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://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2020?applicable_category=Windows&applicable_version=2.1.2.81
CNVD-2021-61088	Graylog 权限许可和访问控制问题漏洞（CNVD-2021-61088）	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.graylog.org/post/announcing-graylog-v4-1-2
CNVD-2021-61407	Mozilla Rust 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rustsec.org/advisories/RUSTSEC-2021-0069.html
CNVD-2021-61760	Vinades NukeViet CMS SQL 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://nukeviet.vn/vi/news/Tin-an-ninh/

			huong-dan-fix-loi-bao-mat-nukeviet-4-va-module-shops-612.html
CNVD-2021-61767	Circutor SGE-PLC1000 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.s21sec.com/

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码等。此外，Siemens、NETGEAR、WordPress 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，获取敏感信息，执行任意代码，导致拒绝服务，缓冲区溢出或堆溢出等。另外，Advantech WebAccess HMI Designer 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞使用专门设计的项目文件，触发基于堆的缓冲区溢出，并在目标系统上执行任意代码。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、 Accela Civic Platform 信息泄露漏洞

验证描述

Accela Civic Platform 是 Accela 公司的应用软件基于云的解决方案使城市系统现代化，以实现土地管理和法规执行、增加公民参与和移动信息访问。

Accela Civic Platform 20.1 之前版本中存在信息泄露漏洞，攻击者可通过修改 contactSeqNumber 值利用该漏洞获取敏感信息。

验证信息

POC 链接：https://packetstormsecurity.com/files/163116/Accela-Civic-Platform-21.1-Insecure-Direct-Object-Reference.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-61769

信息提供者

新华三技术有限公司

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. 福特网站漏洞暴露了内部系统的客户和员工记录

15 日消息，福特网站上的一个漏洞允许访问敏感系统并获取专有数据，如客户数据

库、员工记录、内部机票等。该数据暴露源于 Pega 客户参与系统在福特服务器上运行错误配置。

参考链接：https://www.bleepingcomputer.com/news/security/ford-bug-exposed-customer-and-employee-records-from-internal-systems/

2. 微软修补 3 个零日漏洞

微软于修补了 44 个安全漏洞，当中有 7 个被列为重大（Critical）漏洞。另有 3 个已被公开的漏洞，包含尚未被利用的 CVE-2021-36942 与涉及 Print Spooler 的新漏洞 CVE-2021-36936，以及已经遭到利用的 CVE-2021-36948。

参考链接：https://www.ithome.com.tw/news/146135

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