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 26 日-2021 年 08 月 01 日　　2021 年第 30 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 484 个，其中高危漏洞 131 个、中危漏洞 299 个、低危漏洞 54 个。漏洞平均分值为 5.69。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 44%），其中互联网上出现“SourceCodester E-Commerce Website 跨站脚本漏洞、SourceCodester Travel Management System 文件上传漏洞”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 4248 个，与上周（4935 个）环比减少 14%。

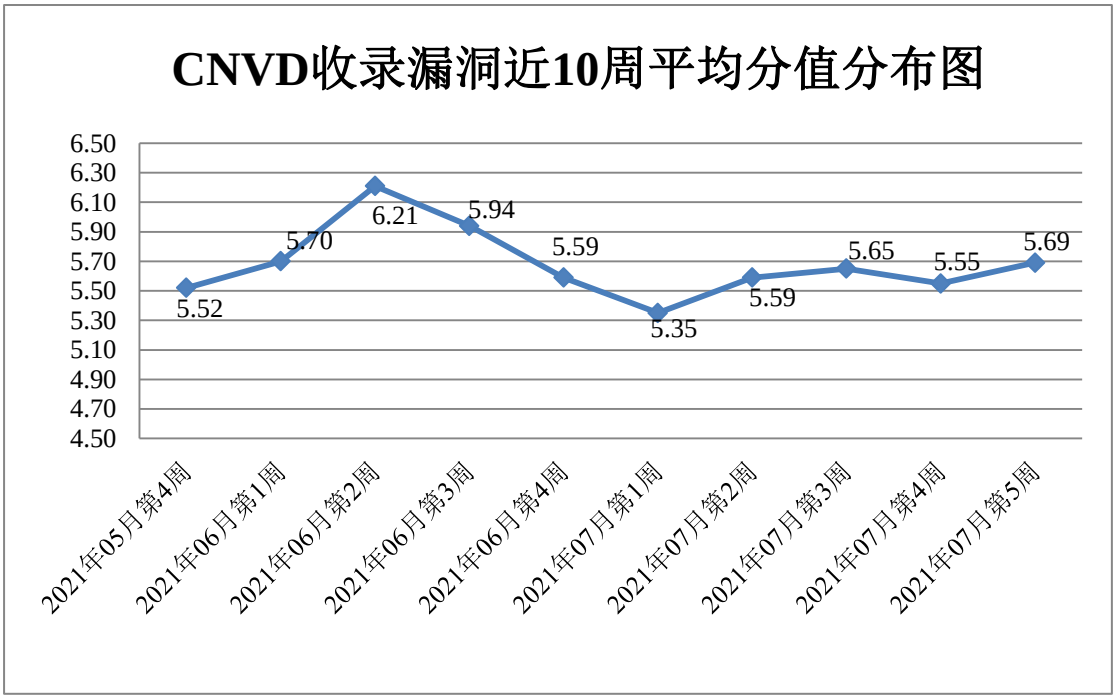

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 32 起，向基础电

信企业通报漏洞事件 68 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 663 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 40 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 33 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、淄博闪灵网络科技有限公司、珠海玖时光科技有限公司、中信建投证券股份有限公司、中科博华信息科技有限公司、中集智能科技有限公司、浙江中控技术股份有限公司、浙江核新同花顺网络信息股份有限公司、浙江大华技术股份有限公司、优刻得科技股份有限公司、用友网络科技股份有限公司、扬中邦宁网络科技有限公司、亚信科技控股有限公司、星云海数字科技股份有限公司、新岸线科技集团有限公司、西门子（中国）有限公司、西安新软信息科技有限公司、西安网卓信息技术有限公司（凯天网络）、西安华天协同信息技术有限公司、武汉舜通智能科技有限公司、武汉爱码农网络科技有限公司、伟乐视讯科技股份有限公司、天津创享信息科技有限公司、天地伟业技术有限公司、泰科安全设备（上海）有限公司、太行保险经纪有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、深圳市因格智能科技有限公司、深圳市迅雷网络技术有限公司、深圳市美科星通信技术有限公司、深圳市朗驰欣创科技股份有限公司、深圳市锟铻科技有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳华望技术有限公司、上海万欣计算机科技有限公司、上海牛迈网络科技有限公司、上海泛微网络科技股份有限公司、上海博瑞康数字科技有限公司、上海博达数据通信有限公司、上海贝锐信息科技股份有限公司、上海安达通信息安全技术股份有限公司、山西邮电建设工程有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、厦门科拓通讯技术股份有限公司、厦门计讯物联科技有限公司、赛诺联合医疗科技（北京）有限公司、任子行网络技术股份有限公司、普联技术有限公司、欧姆龙自动化（中国）有限公司、宁波万由电子科技有限公司、南京科远自动化集团股份有限公司、南京科远智慧科技集团股份有限公司、迈普通信技术股份有限公司、联想（北京）有限公司、理光（中国）投资有限公司、浪潮集团、兰州市轨道交通有限公司、酷艺文化科技发展有限公司、科大讯飞股份有限公司、傑立資訊事業有限公司、江苏沃叶软件有限公司、江苏朗拓健康科技有限公司、嘉兴想天信息科技有限公司、嘉兴市信达电子科技有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南强智科技发展有限公司、湖南翱云网络科技有限公司、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、汉王科技股份有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、广州网易计算机系统有限公司、广州万彩信息技术有限公司、广州图创计算机软件开发有限公司、广州市九安智能技术股份有限公司、广州市奥威亚电子科技有限公司、广州国微软件科技有限公司、广联达科技股份

有限公司、广东南方数码科技股份有限公司、光软件系统有限公司、福建福昕软件开发股份有限公司、大唐电信科技股份有限公司、大连理工计算机控制工程有限公司、郴州帝云网络科技有限公司、畅捷通信息技术股份有限公司、北京卓软在线信息技术有限公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京云帆互联科技有限公司、北京用友政务软件股份有限公司、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、北京网康科技有限公司、北京万维盈创科技发展有限公司、北京圣博润高新技术股份有限公司、北京润尼尔网络科技有限公司、北京巧巧时代网络科技有限公司、北京理正软件股份有限公司、北京火绒网络科技有限公司、北京慧聪建设信息咨询有限公司、北京和信创天科技股份有限公司、北京和欣运达科技有限公司、北京汉王圣博科技有限公司、北京国炬信息技术有限公司、北京东云创达科技有限公司、北京百卓网络技术有限公司、爱普生（中国）有限公司、Angel 工作室网络网络科技有限公司、阿里巴巴集团安全应急响应中心、百度安全应急响应中心、易优模板网、若依、巡云轻论坛系统、小说精品屋、成都零起飞网络、YimaoAdmin、XnSoft、Vpon、seacms、Santesoft、Phpcms、PanDownload、OctoPrint、NETGEAR、MacCMS、Jupyter、iBall、HuCart、HongCMS、EZB Systems, Inc.、Dreamer cms 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，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、北京数字观星科技有限公司、北京天融信网络安全技术有限公司、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、北京华顺信安科技有限公司、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、联想全球安全实验室、杭州海康威视数字技术股份有限公司、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、河南信安世纪科技有限公司、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、上海纽盾科技股份有限公司、南京众智维信息科技有限公司、安徽长泰信息安全服务有限公司、河南灵创电子科技有限公司、中国电信股份有限公司网络安全产品运营中心、北京天地和兴科技有限公司、北京安帝科技有限公司、武汉明嘉信信息安全检测评估有限公司、广东蓝爵网络安全技术股份有限公司、重庆贝特计算机系统工程有限公司、山东新潮信息技术有限公司、上海市信息安全测评认证中心、浙江大华技术股份有限公司、北京远禾科技有限公司、贵州多彩宝互联网服务有限公司、重庆都会信息科技有限公司、泰山信息科技有限公司、杭州迪普科技股份有限公司、北京顶象技术有限公司、中安网盾（广州）信息科技有限公司、江苏保旺达软件技术有限公司、江西古礼月信息技术有限公司、上海嘉韦思信息技术有限公司、中移（杭州）信息技术有限公司、四川赛虎科技有限公司、

深圳市魔方安全科技有限公司、亚信科技（成都）有限公司、南京树安信息技术有限公司及其他个人白帽子向 CNVD 提交了 4248 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 1814 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）	743	743
上海交大	566	566
奇安信网神（补天平台）	505	505
哈尔滨安天科技集团股份有限公司	262	3
北京神州绿盟科技有限公司	208	7
北京数字观星科技有限公司	198	2
远江盛邦（北京）网络安全科技股份有限公司	140	140
北京天融信网络安全技术有限公司	121	24
恒安嘉新（北京）科技股份公司	106	0
新华三技术有限公司	82	0
北京启明星辰信息安全技术有限公司	72	11
华为技术有限公司	69	0
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	59	0
北京安信天行科技有限公司	50	50
西安四叶草信息技术有限公司	11	11

北京奇虎科技有限公司	8	8
南京联成科技发展股份有限公司	4	4
北京信息安全测评中心	2	2
北京知道创宇信息技术股份有限公司	1	0
山东云天安全技术有限公司	279	279
北京华顺信安科技有限公司	259	1
北京山石网科信息技术有限公司	249	249
北京信联科汇科技有限公司	249	249
联想全球安全实验室	243	4
杭州海康威视数字技术股份有限公司	137	137
浙江木链物联网科技有限公司	90	90
北京华云安信息技术有限公司	85	85
河南信安世纪科技有限公司	71	71
山东泽鹿安全技术有限公司	61	61
江西省掌控者信息安全技术有限公司	44	44
上海纽盾科技股份有限公司	35	35
南京众智维信息科技有限公司	35	35
安徽长泰信息安全服	33	33

务有限公司		
河南灵创电子科技有限公司	28	28
中国电信股份有限公司网络安全产品运营中心	20	1
北京天地和兴科技有限公司	18	18
北京安帝科技有限公司	15	15
武汉明嘉信信息安全检测评估有限公司	14	14
广东蓝爵网络安全技术股份有限公司	12	12
重庆贝特计算机系统工程有限公司	10	10
山东新潮信息技术有限公司	8	8
上海市信息安全测评认证中心	7	7
浙江大华技术股份有限公司	6	6
北京远禾科技有限公司	3	3
贵州多彩宝互联网服务有限公司	3	3
重庆都会信息科技有限公司	2	2
泰山信息科技有限公司	2	2
杭州迪普科技股份有限公司	1	1
北京顶象技术有限公司	1	1

中安网盾（广州）信息科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
江西古礼月信息技术有限公司	1	1
上海嘉韦思信息技术有限公司	1	1
中移（杭州）信息技术有限公司	1	1
四川赛虎科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
亚信科技（成都）有限公司	1	1
南京树安信息技术有限公司	1	1
CNCERT 宁夏分中心	12	12
CNCERT 浙江分中心	7	7
CNCERT 西藏分中心	4	4
CNCERT 山东分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 四川分中心	1	1
个人	633	633
报送总计	5895	4248

本周漏洞按类型和厂商统计

本周，CNVD 收录了 484 个漏洞。应用程序 213 个，WEB 应用 181 个，网络设备（交换机、路由器等网络端设备）45 个，数据库 19 个，智能设备（物联网终端设备）18 个，操作系统 4 个，安全产品 4 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	213

WEB 应用	181
网络设备（交换机、路由器等网络端设备）	45
数据库	19
智能设备（物联网终端设备）	18
操作系统	4
安全产品	4

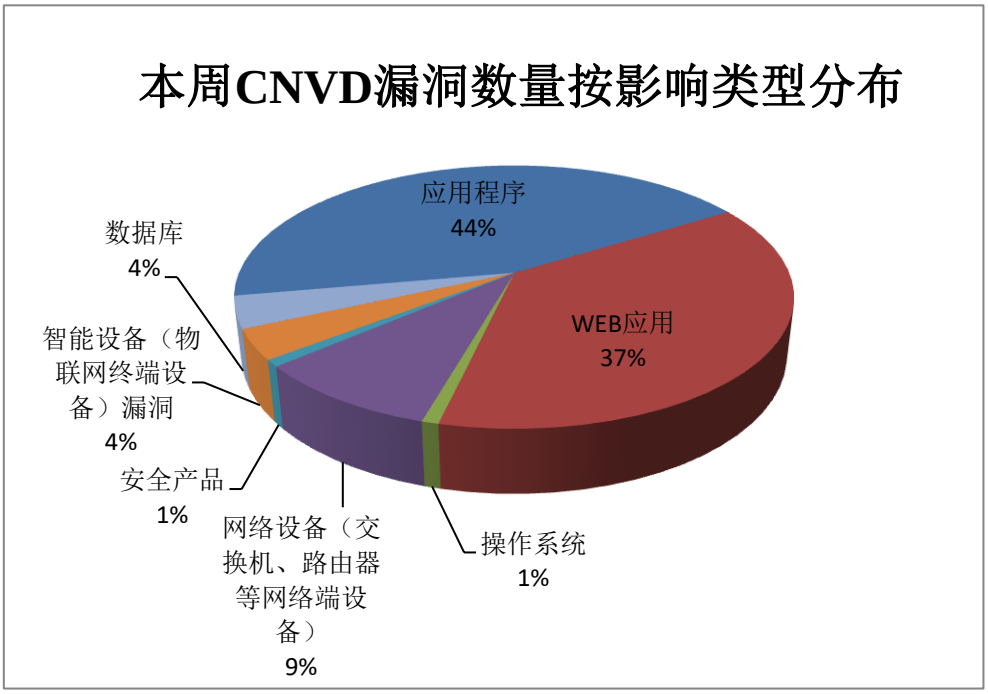

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、NCH Software、NETGEAR 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	Oracle	62	13%
2	NCH Software	30	6%
3	NETGEAR	20	4%
4	Google	20	4%
5	Adobe	15	3%
6	北京鼎软科技有限公司	15	3%
7	Atlassian	13	3%
8	Mozilla	13	3%
9	IBM	11	2%
10	其他	285	59%

本周行业漏洞收录情况

本周，CNVD 收录了 37 个电信行业漏洞，8 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Buffalo WSR-2533DHPL2 和 WSR-2533DHP3 存在路径遍历漏洞、Google Chrome Android intents 安全绕过漏洞、RainbowFish PacsOne Server 访问控制错误漏洞”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/

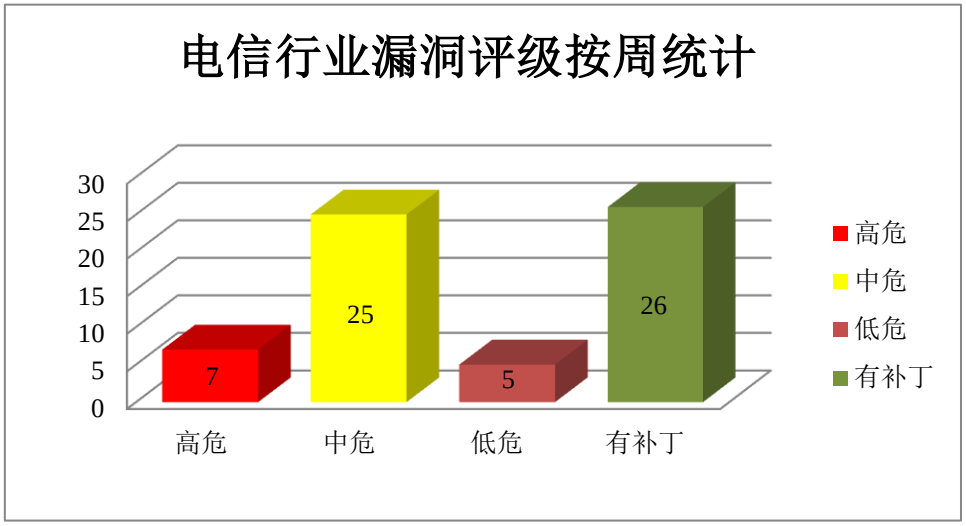

图 3 电信行业漏洞统计

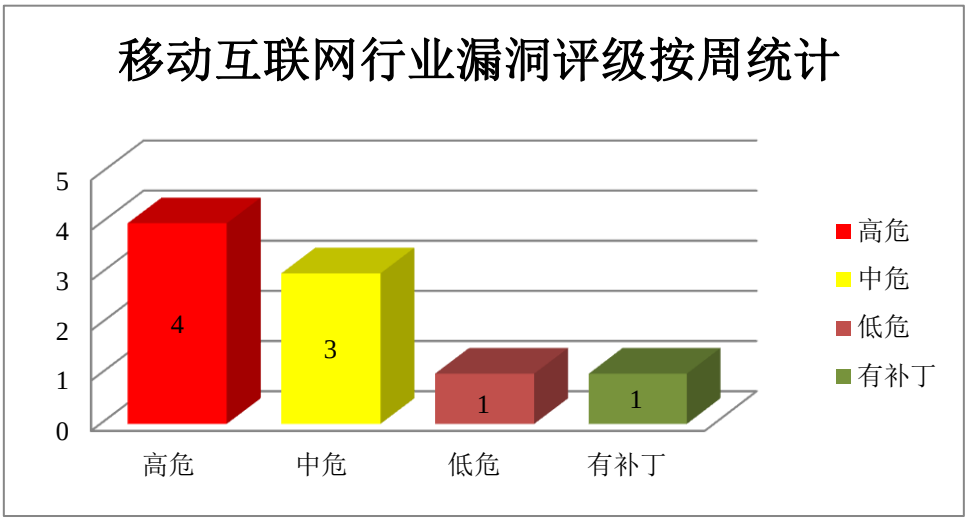

图 4 移动互联网行业漏洞统计

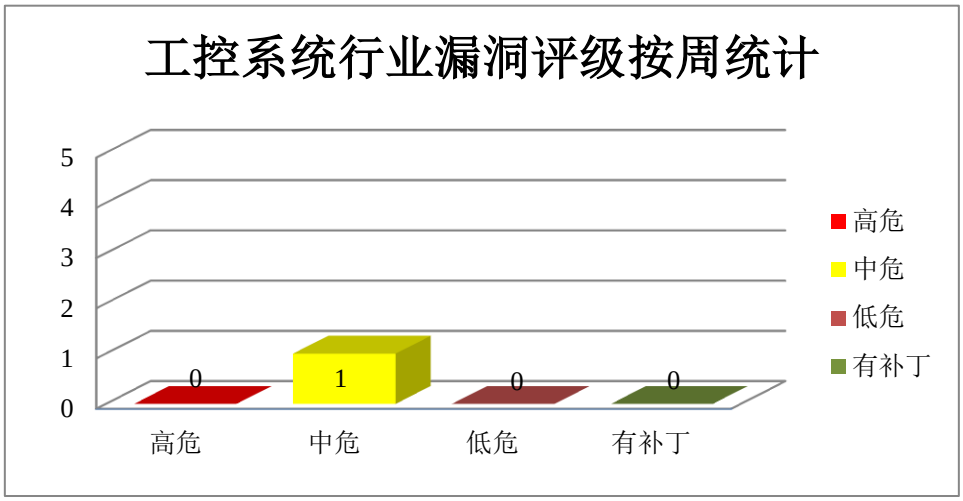

图 5 工控系统行业漏洞统计

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

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在代码执行漏洞，攻击者可利用漏洞在系统上执行任意代码或造成拒绝服务情况。

CNVD 收录的相关漏洞包括：Google Chrome sensor handling 代码执行漏洞、Google Chrome dialog box 代码执行漏洞、Google Chrome DevTools 代码执行漏洞（CNVD-2021-55926、CNVD-2021-55931）、Google Chrome UI 框架代码执行漏洞、Google Chrome Autofill 代码执行漏洞、Google Chrome GPU 代码执行漏洞、Google Chrome 协议处理代码执行漏洞。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-2021-55922

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55921

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55926

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55931

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55928

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55935

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55934

https://www.cnvd.org.cn/flaw/show/CNVD-2021-55933

2、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，在目标系统上执行任意代码，导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 缓冲区溢出漏洞（CNVD-2021-54699、CNVD-2021-54700、CNVD-2021-54702）、Mozilla Firefox UI 欺骗漏洞、Mozilla Firefox 资源管理错误漏洞（CNVD-2021-54704）、Mozilla Firefox 数据伪造问题漏洞（CNVD-2021-54703）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2021-54706）、Mozilla Firefox WebGL 释放后重用漏洞。其中，“Mozilla Firefox WebGL 释放后重用漏洞”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-2021-54699

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54700

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54705

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54704

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54703

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54702

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54706

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54710

3、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle VM VirtualBox 是一款针对 x86 系统的跨平台虚拟化软件。Oracle PeopleSoft Enterprise PeopleTools 提供了一个支持 PeopleSoft 应用程序的开发和运行时的全面的开发工具集。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权访问数据，导致 MySQL 服务器挂起或频繁重复崩溃。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2021-54672、CNVD-2021-54675、CNVD-2021-54674、CNVD-2021-54673、CNVD-2021-54676）、Oracle VM VirtualBox 未授权访问漏洞（CNVD-2021-54713、CNVD-2021-54712）、Oracle PeopleSoft Enterprise PeopleTools 未授权访问漏洞（CNVD-2021-54719）。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-2021-54672

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54675

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54674

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54673

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54676

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54713

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54712

https://www.cnvd.org.cn/flaw/show/CNVD-2021-54719

4、NETGEAR 产品安全漏洞

NETGEAR R6700、NETGEAR R7800、NETGEAR R6250、NETGEAR R8300、NETGEAR R9000、NETGEAR WNDR4500、NETGEAR WNR2020 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR D8500 是一款无线调制解调器。NETGEAR D6100 是一款无线调制解调器。NETGEAR D6200 是一款无线调制解调器。NETGEAR D7000 是一款无线调制解调器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件，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 产品跨站请求伪造漏洞（CNVD-2021-57165）、多款 NETGEAR 产品拒绝服务漏洞（CNVD-2021-57164）、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-57170、CNVD-2021-57173、CNVD-2021-57172、CNVD-2021-57171、CNVD-2021-57174）、多款 NETGEAR 产品输入验证错误漏洞（CNVD-2021-57176）。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-2021-57165
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57164
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57170
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57173
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57172
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57171
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57176
https://www.cnvd.org.cn/flaw/show/CNVD-2021-57174

5、Realtek RTL8710 缓冲区溢出漏洞（CNVD-2021-56811）

Realtek RTL8710 是中国台湾瑞昱半导体（Realtek）公司的一款物联网微控制器。本周，Realtek RTL8710 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过"emcpy "功能远程执行代码。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-2021-56811

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-2021-55168	Helpcom 输入验证错误漏洞	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://hc119.com/index.jsp?go=on
CNVD-2021-	Miniaudio 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时

55177			关注更新：https://github.com/mackron/miniaudio/commit/8234df87c9268507847e0033280067bade9a57a1
CNVD-2021-55176	ZOHO ManageEngine ADSelfService Plus 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://www.manageengine.com/products/self-service-password/release-notes.html#6102
CNVD-2021-55192	IBM i2 iBase 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://www.ibm.com
CNVD-2021-55897	Aruba ClearPass Policy Manager 服务器端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-009.txt
CNVD-2021-55907	NCH IVM Attendant 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.nch.com.au/ivm/index.html
CNVD-2021-55927	Google Chrome Android intents 安全绕过漏洞	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-2021-55975	Adobe Acrobat/Reader 堆缓冲区溢出漏洞（CNVD-2021-55975）	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/acrobat/apsb21-51.html
CNVD-2021-56797	Buffalo WSR-1166DHP3 和 WSR-1166DHP4 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.buffalo.jp/news/detail/20210531-01.html
CNVD-2021-57227	Victor CMS 任意文件上传漏洞	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/TCSWT/Victor-CMS/blob/main/README.md

小结：本周，Google 产品被披露存在代码执行漏洞，攻击者可利用漏洞在系统上执行任意代码或造成拒绝服务情况。此外，Mozilla、Oracle、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，读取任意文件，在目标系统上执行任意代码，导致拒绝服务攻击等。另外，Realtek RTL8710 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过"emcpy"功能远程执行代码。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、SourceCodester Travel Management System 文件上传漏洞

验证描述

SourceCodester Travel Management System 是一个应用软件。一个自动化系统，旨在帮助客户轻松检查他们的包裹详细信息，同时帮助旅行公司在线跟踪包裹。

SourceCodester Travel Management System v1.0 存在文件上传漏洞，攻击者可利用该漏洞通过将文件上传到 updatepackage.php 来执行任意代码。

验证信息

POC 链接：https://github.com/BigTiger2020/Travel-Management-System/blob/main/Travel%20Management%20System.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-55185

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. 福昕 PDF 阅读器、编辑器中存在多个安全漏洞

福昕 PDF 阅读器和 PDF 编辑器应用程序已进行了安全更新，以解决包括远程代码执行在内的多个漏洞。

参考链接：https://www.securityweek.com/foxit-plugs-multiple-security-holes-pdf-reader-editor

2. Apple 修复了 CVE-2021-30807 漏洞，这是今年第 13 个零日漏洞

Apple 发布了一个安全更新，解决了 macOS 和 iOS 中的 CVE-2021-30807 漏洞，该漏洞可能已被积极利用来传播恶意软件。

参考链接：https://securityaffairs.co/wordpress/120576/security/apple-cve-2021-30807-zero-day.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