国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 04 月 19 日-2021 年 04 月 25 日　　2021 年第 16 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 688 个，其中高危漏洞 204 个、中危漏洞 416 个、低危漏洞 68 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 361 个（占 52%），其中互联网上出现“Wcms 服务端请求伪造漏洞、LavaLite 跨站脚本漏洞（CNVD-2021-29738）”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 2761 个，与上周（3828 个）环比减少 28%。

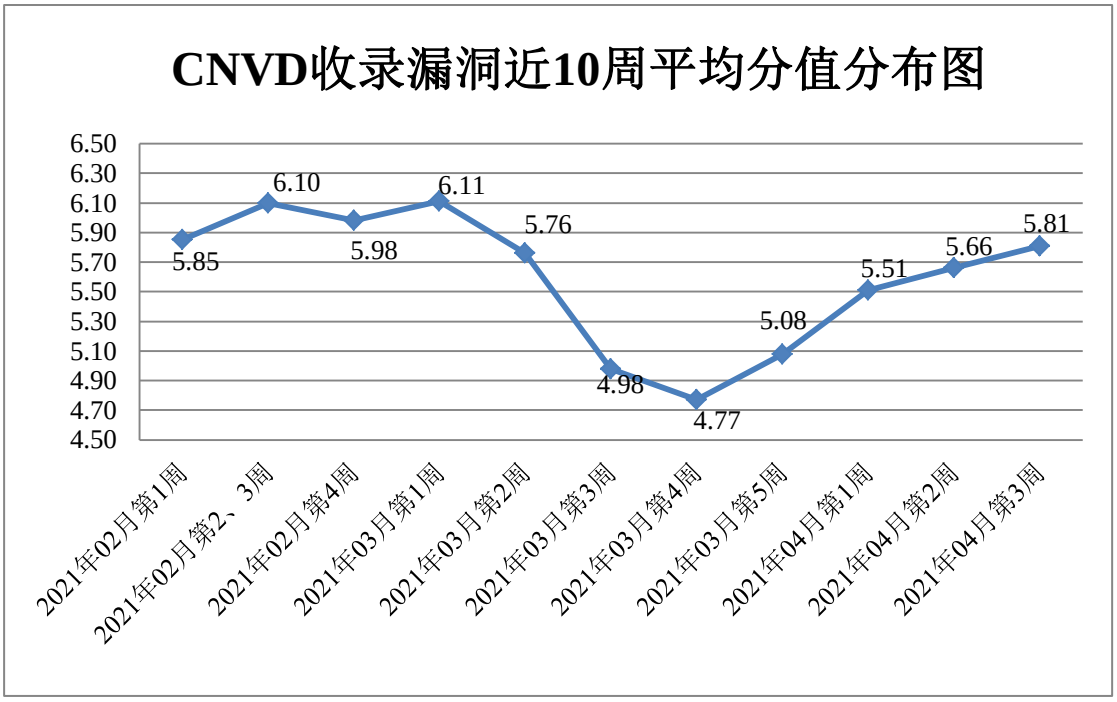

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 起，向基础电

信企业通报漏洞事件 19 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 398 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 60 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 43 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、重庆软航科技有限公司、中新网络信息安全股份有限公司、中建智云网络通信有限公司、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、西安众邦网络科技有限公司、西安瑞友信息技术资讯有限公司、武汉舜通智能科技有限公司、武汉深之度科技有限公司、无锡开云信息技术有限公司、统信软件技术有限公司、松下电器（中国）有限公司、深圳市圆梦云科技有限公司、深圳市鑫金浪电子有限公司、深圳市腾狐物联科技有限公司、深圳市普燃计算机软件科技有限公司、深圳市联软科技股份有限公司、深圳市磊科实业有限公司、深圳市吉祥腾达科技有限公司、深圳市汇川技术股份有限公司、深圳市河辰通讯技术有限公司、深圳市朝恒辉网络科技有限公司、深圳华视美达信息技术有限公司、深圳鼎信通达股份有限公司、上海泰彼信息科技有限公司、上海求创科技有限公司、上海斐讯数据通信技术有限公司、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、上海步科自动化股份有限公司、熵基科技股份有限公司、山东国子软件股份有限公司、山大鲁能信息科技有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、厦门海为科技有限公司、锐捷网络股份有限公司、普联技术有限公司、南京三商电脑软件开发有限公司、南京帆软软件有限公司、浪潮集团有限公司、蓝网科技股份有限公司、居易科技股份有限公司、江苏易索电子科技股份有限公司、江苏三恒科技股份有限公司、江苏汉思未来信息科技有限公司、湖南潭州教育网络科技有限公司、湖南翱云网络科技有限公司、湖北点点点科技有限公司、河南盘古科技发展有限公司、杭州雄迈信息技术有限公司、杭州思福迪信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州法源软件开发有限公司、杭州迪普科技股份有限公司、汉柏科技有限公司、广州网易计算机系统有限公司、广州市乐天科技有限公司、广州山锋测控技术有限公司、广州齐博网络科技有限公司、广州璐华信息技术有限公司、广州京思顿电子科技有限公司、广州红帆科技有限公司、广东南方数码科技股份有限公司、谷歌公司、福建福昕软件开发股份有限公司、帝兴软件开发有限公司、大麦科技发展有限公司、成都青软青之软件有限公司、成都飞鱼星科技股份有限公司、成都爱诚科技有限公司、北京筑龙信息技术有限责任公司、北京致远互联软件股份有限公司、北京易联易通科技有限公司、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、北京世纪长秋科技有限公司、北京世纪超星信息技术发展有限责任公司、北京玛格泰克科技发展有限公司、北京猎鹰安全科技有限公司、北京金万维科技有限公司、北京国炬信息技术有限公司、北京

北信源软件股份有限公司、北京百度网讯科技有限公司、安徽科迅教育装备有限公司、施耐德电气、里客云科技、邢台智工软件服务中心、云收藏、鱼跃 CMS、The Apache Software Foundation、SEMCMS、Seacms、Oracle、MacCMS、Kyan、HYBBS、Cszcms、cisco、AKCMS 和 ABBYY。

本周，CNVD 发布了《Oracle 发布 2021 年 4 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6356

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、北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、杭州海康威视数字技术股份有限公司、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、河南信安世纪科技有限公司、武汉明嘉信信息安全检测评估有限公司、小安（北京）科技有限公司、安徽长泰信息安全服务有限公司、北京山石网科信息技术有限公司、重庆贝特计算机系统工程有限公司、杭州木链物联网科技有限公司、山东泽鹿安全技术有限公司、北京天地和兴科技有限公司、山东新潮信息技术有限公司、北京安帝科技有限公司、浙江大华技术股份有限公司、中资网络信息安全科技有限公司、京东云安全、北京墨云科技有限公司、日照天鉴网络科技有限公司、国网山东省电力公司、浙江御安信息技术有限公司、北京零零信安科技有限公司、福建省海峡信息技术有限公司、北京安华金和科技有限公司、四川哨兵信息科技有限公司、平安银河实验室、工业信息安全（四川）创新中心有限公司、北京远禾科技有限公司、中国银行、深圳开源互联网安全技术有限公司、长春嘉诚信息技术股份有限公司、武汉安域信息安全技术有限公司、广州百蕴启辰科技有限公司、杭州美创科技有限公司、广东东方思维科技有限公司、深圳市魔方安全科技有限公司及其他个人白帽子向 CNVD 提交了 2761 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）、上海交大和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1257 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）	712	712
上海交大	456	456
北京天融信网络安全技术有限公司	443	3
北京神州绿盟科技有	321	14

限公司		
哈尔滨安天科技集团股份有限公司	262	0
华为技术有限公司	232	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）	131	131
北京数字观星科技有限公司	126	0
深信服科技股份有限公司	120	15
斗象科技（漏洞盒子）	89	89
恒安嘉新（北京）科技股份公司	70	0
新华三技术有限公司	56	0
北京启明星辰信息安全技术有限公司	55	0
远江盛邦（北京）网络安全科技股份有限公司	18	18
北京知道创宇信息技术股份有限公司	9	4
杭州安恒信息技术股份有限公司	5	5
西安四叶草信息技术有限公司	2	2
北京信联科汇科技有限公司	218	218
杭州海康威视数字技术股份有限公司	134	134
中国电信股份有限公司网络安全产品运营中心	41	21
河南灵创电子科技有限公司	33	33
河南信安世纪科技有限公司	32	32
武汉明嘉信信息安全检测评估有限公司	26	26
小安（北京）科技有限公司	20	20
安徽长泰信息安全服	16	16

务有限公司		
北京山石网科信息技术有限公司	14	14
重庆贝特计算机系统工程有限公司	14	14
杭州迪普科技股份有限公司	13	0
杭州木链物联网科技有限公司	13	13
山东泽鹿安全技术有限公司	11	11
北京天地和兴科技有限公司	10	10
山东新潮信息技术有限公司	8	8
北京安帝科技有限公司	8	8
浙江大华技术股份有限公司	5	5
中资网络信息安全科技有限公司	5	5
京东云安全	5	5
北京墨云科技有限公司	4	4
日照天鏊网络科技有限公司	3	3
国网山东省电力公司	3	3
浙江御安信息技术有限公司	3	3
北京零零信安科技有限公司	3	3
福建省海峡信息技术有限公司	3	3
北京安华金和科技有限公司	2	2
四川哨兵信息科技有限公司	2	2
平安银河实验室	2	2
工业信息安全（四川）创新中心有限公司	2	2
北京远禾科技有限公司	1	1
中国银行	1	1

深圳开源互联网安全技术有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
武汉安域信息安全技术有限公司	1	1
广州百蕴启辰科技有限公司	1	1
杭州美创科技有限公司	1	1
广东东方思维科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
CNCERT 贵州分中心	6	6
CNCERT 山西分中心	4	4
CNCERT 河北分中心	1	1
CNCERT 海南分中心	1	1
个人	671	671
报送总计	4452	2761

本周漏洞按类型和厂商统计

本周，CNVD 收录了 688 个漏洞。应用程序 306 个，WEB 应用 223 个，网络设备（交换机、路由器等网络端设备）68 个，操作系统 55 个，安全产品 16 个，数据库 11 个，智能设备（物联网终端设备）9 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	306
WEB 应用	223
网络设备（交换机、路由器等网络端设备）	68
操作系统	55
安全产品	16
数据库	11
智能设备（物联网终端设备）	9

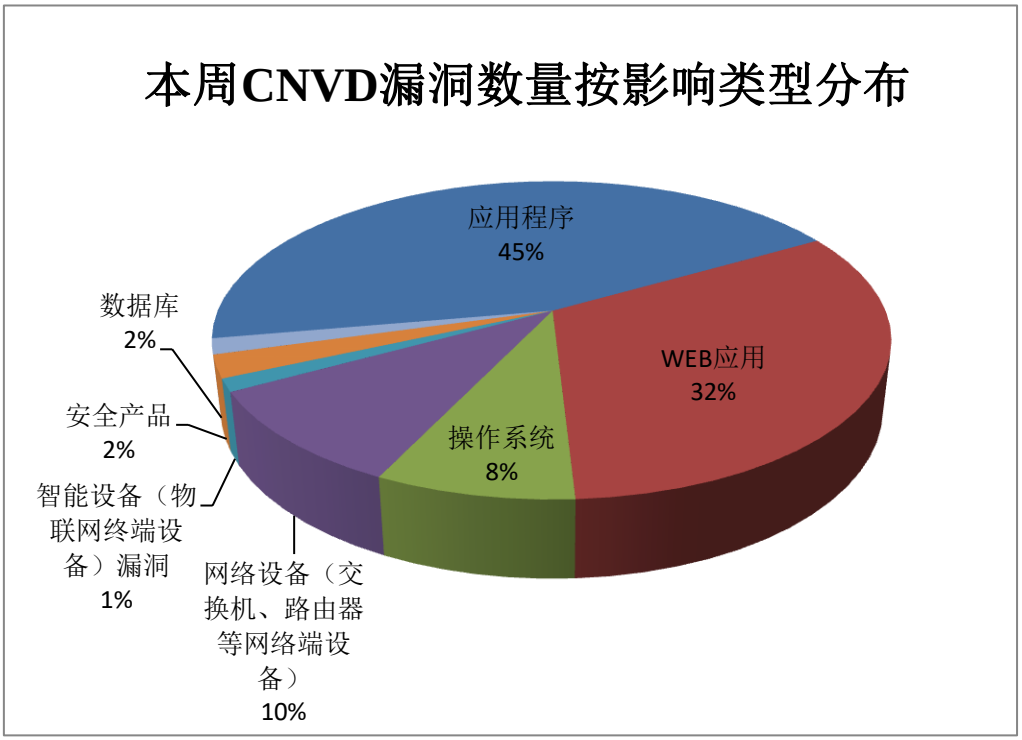

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、Oracle、《中国学术期刊（光盘版）》电子杂志社有限公司等多家厂商的产品，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	Mozilla	36	5%
2	Oracle	31	5%
3	《中国学术期刊（光盘版）》电子杂志社有限公司	28	4%
4	GPAC	24	4%
5	WordPress	22	3%
6	Samsung	24	3%
7	Microsoft	20	3%
8	Google	19	3%
9	SEMCMS	17	2%
10	其他	467	68%

本周行业漏洞收录情况

本周，CNVD 收录了 69 个电信行业漏洞，30 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，“Eaton Intelligent Power Manager 远程代码执行漏洞、Google Android 权限提升漏洞（CNVD-2021-30158）、D-Link DIR-878 栈缓冲区溢出漏洞、IBM WebSphere Application Server 外部实体注入漏洞”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/

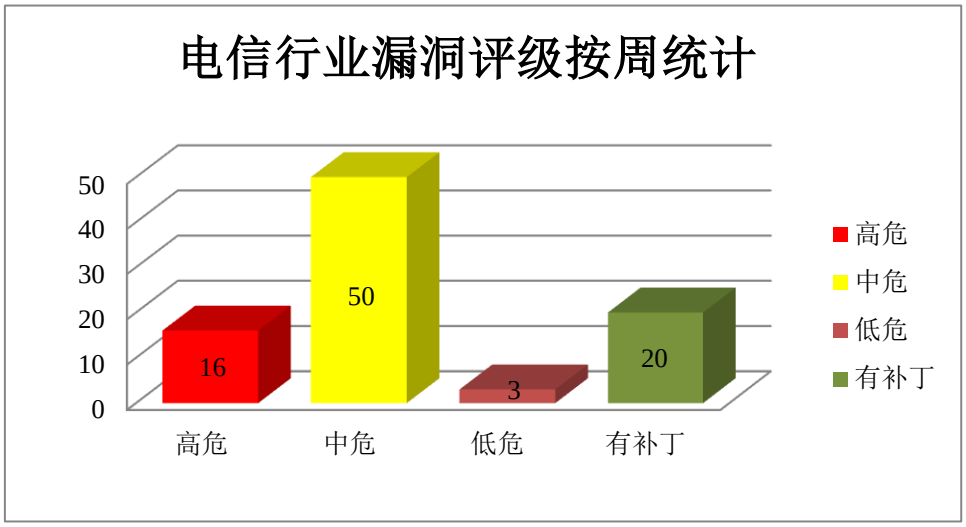

图 3 电信行业漏洞统计

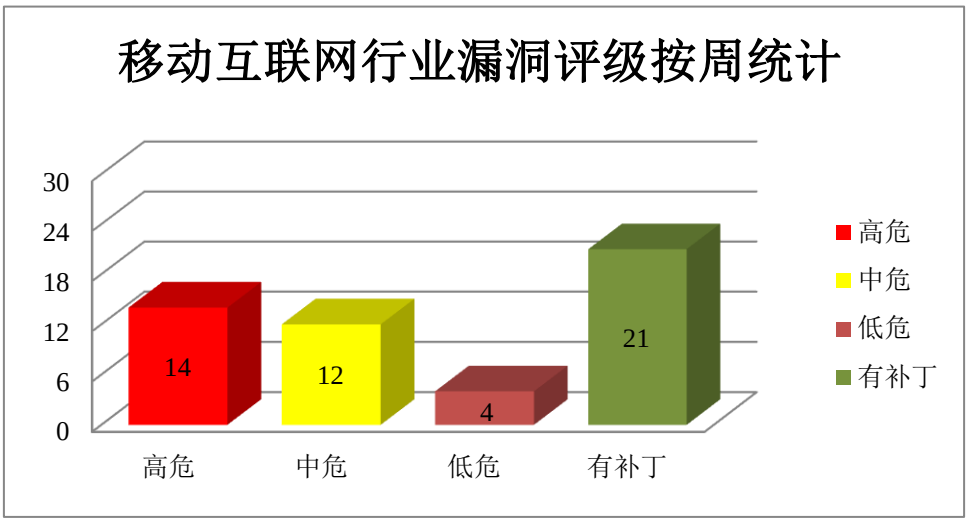

图 4 移动互联网行业漏洞统计

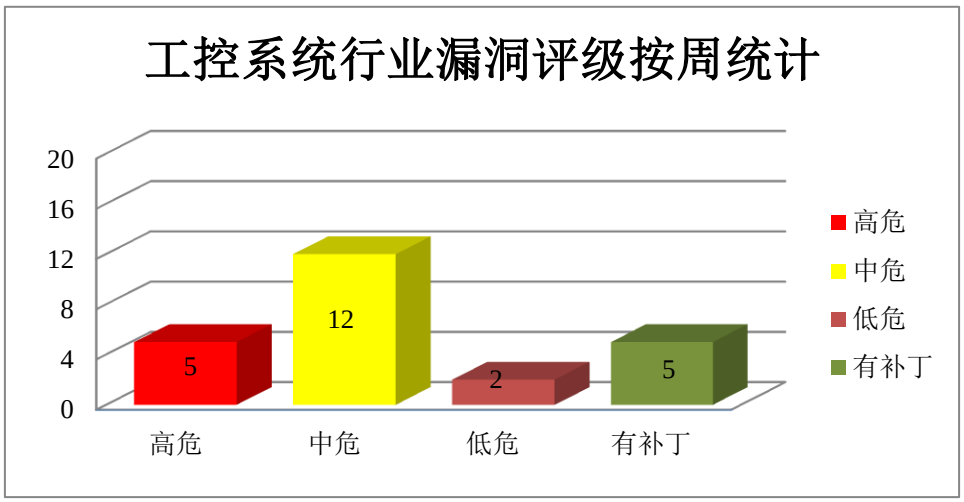

图 5 工控系统行业漏洞统计

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、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。Windows Kernel 是其中的一个 Windows 系统内核。Windows Installer 是其中的一个基于 Windows 系统的工具组件，主要用于管理和配置软件服务。Microsoft Windows Runtime（.net framework）是美国微软（Microsoft）公司的一款 Windows 操作系统中必要的功能支持库。Microsoft Visual Studio Code 是美国微软（Microsoft）公司的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。

CNVD 收录的相关漏洞包括：Microsoft Windows WalletService 权限提升漏洞（CNVD-2021-29542）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2021-29541、CNVD-2021-29550）、Microsoft Windows Installer 权限提升漏洞（CNVD-2021-29546）、Microsoft Windows Runtime 权限提升漏洞（CNVD-2021-29549）、Microsoft Visual Studio 代码执行漏洞（CNVD-2021-29877、CNVD-2021-29880、CNVD-2021-29995）。其中，“Microsoft Windows Kernel 权限提升漏洞（CNVD-2021-29541、CNVD-2021-29550）”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-2021-29542
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29541
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29546
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29550
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29549
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29877
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29880
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29995

2、Adobe 产品安全漏洞

Adobe Bridge 是 Adobe 公司推出的一款免费数字资产管理应用程序。Adobe Digital Editions（DE）是美国奥多比（Adobe）公司的一套电子书阅读管理软件。该软件支持打开、阅读和管理 PDF、XML、Flash 等格式的文件。Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境

和脚本语言。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，写入任意文件系统，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Bridge 越界写入漏洞（CNVD-2021-30417、CNVD-2021-30416）、Adobe Digital Editions 权限提升漏洞、Adobe Bridge 越界读取漏洞（CNVD-2021-30421）、Adobe Bridge 内存破坏漏洞（CNVD-2021-30419、CNVD-2021-30418）、Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-30425）、Adobe ColdFusion 跨站脚本漏洞（CNVD-2021-30491）。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-2021-30417
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30416
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30415
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30421
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30419
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30418
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30425
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30491

3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。System 是其中的一个系统组件。VPN 是其中的一个 VPN（虚拟专用网络）组件。Email 是其中的一个电子邮件组件。Framework 是其中的一个 Android 框架组件。Broadcom Bluetooth 是其中的一个蓝牙组件。Wi-Fi 是其中的一个无线上网组件。USB driver 是其中的一个通用串行总线（USB）驱动程序。Bluetooth 是其中的一个蓝牙组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面造成堆破坏，导致应用拒绝服务，获取服务器控制权限等。

CNVD 收录的相关漏洞包括：Google Chrome 释放后重用漏洞（CNVD-2021-30148、CNVD-2021-30147、CNVD-2021-30149、CNVD-2021-30154）、Google Android Framework 权限提升漏洞（CNVD-2021-30152）、Google Android 权限提升漏洞（CNVD-2021-30157、CNVD-2021-30158）、Google Android 拒绝服务漏洞（CNVD-2021-30160）。其中，“Google Android Framework 权限提升漏洞（CNVD-2021-30152）、Google Android 权限提升漏洞（CNVD-2021-30157、CNVD-2021-30158）”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-2021-30148
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30147
https://www.cnvd.org.cn/flaw/show/CNVD-2021-30149

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30154

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30152

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30157

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30160

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30158

4、Oracle 产品安全漏洞

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。本周，上述产品被披露存在输入验证错误漏洞，攻击者可利用漏洞影响机密性，完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 输入验证错误漏洞（CNVD-2021-30524、CNVD-2021-30523、CNVD-2021-30526、CNVD-2021-30525、CNVD-2021-30530、CNVD-2021-30529、CNVD-2021-30528、CNVD-2021-30531）。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-2021-30524

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30523

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30526

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30525

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30530

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30529

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30528

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30531

5、D-Link DIR-816 栈缓冲区溢出漏洞

D-Link DIR-816 是一款无线 AC750 双频路由器。本周，D-Link DIR-816 被披露存在栈缓冲区溢出漏洞。攻击者可通过 s_ip 和 s_mac 字段的长文本输入利用该漏洞导致路由器崩溃。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-2021-30001

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-2021-29470	Micro Focus Operations Bridge Manager 认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://softwaresupport.softwaregrp.com

			/doc/KM03793283
CNVD-2021-29469	SonicWall Global Management System 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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0009
CNVD-2021-29485	Apache DolphinScheduler 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://lists.apache.org/thread.html/rcbe4c248ef0c566e99fd19388a6c92aeef88167286546b675e9b1769%40%3Cdev.dolphinscheduler.apache.org%3E
CNVD-2021-29839	Schneider Electric C-Bus Toolkit 路径遍历漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01
CNVD-2021-29845	WordPress gVectors wpDiscuz plugin SQL 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://wpdiscuz.com/community/news/security-vulnerability-issue-in-5-3-5-please-udate/
CNVD-2021-29991	Juniper Networks Junos OS 存在未名漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11161&cat=SIRT_1&actp=LIST
CNVD-2021-30151	Google Android Framework 权限提升漏洞（CNVD-2021-30151）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2020-12-01
CNVD-2021-30577	Mozilla Rust linked-hash-map 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://rustsec.org/advisories/RUSTSEC-2020-0026.html
CNVD-2021-30591	Eaton Intelligent Power Manager Eval 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://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf
CNVD-2021-30590	Helpcom 授权问题漏洞	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://hc119.com/install.jsp

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。此外，Adobe、Google、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面造成堆破坏，获取敏感信息，写入任意文件系统，执行任意代码，导致应用拒绝服务等。另外，D-Link DIR-816 被披露存在栈缓冲区溢出漏洞。攻击者可通过 s_ip 和 s_mac 字段的长文本输入利用该漏洞导致路由器崩溃。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、LavaLite 跨站脚本漏洞（CNVD-2021-29738）

验证描述

Lavalite 是一款使用 Laravel 框架开发的开源内容管理系统。

LavaLite 5.8.0 版本存在跨站脚本漏洞。攻击者可通过“地址”字段利用该漏洞进行跨站脚本攻击。

验证信息

POC 链接：https://github.com/418sec/huntr/tree/staging/bounties/packagist/lavalite/cms/3

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-29738

信息提供者

华为技术有限公司

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. Facebook 被爆新漏洞：可收集用户的电子邮件信息

本月早些时候，有人在黑客论坛上放出了一个拥有 5.3 亿 Facebook 用户个人信息的数据集。随后该公司承认存在本次数据泄漏，但表示不会通知在该漏洞中受到影响的用户。虽然 Facebook 表示已经修复了之前允许黑客从该社交平台上刮取数据的漏洞，不过一名安全研究人员发现了另一个漏洞。该漏洞允许黑客从 Facebook 上刮取电子邮件地址。

参考链接：https://www.chinaz.com/2021/0422/1240455.shtml

2. 智能炸锅中发现了远程执行代码漏洞

研究人员在 Cosori 智能空气炸锅中发现了两个 RCE 漏洞。该产品是一个 Wi-Fi 连接的厨房产品，可以用过互联网让用户远程控制烹饪温度、时间和设置。

参考链接：https://www.zdnet.com/article/remote-code-execution-vulnerabilities-uncovered-in-smart-air-fryer/

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