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 19 日-2021 年 07 月 25 日　　2021 年第 29 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 594 个，其中高危漏洞 162 个、中危漏洞 375 个、低危漏洞 57 个。漏洞平均分值为 5.55。本周收录的漏洞中，涉及 0day 漏洞 301 个（占 51%），其中互联网上出现“LJCMS SQL 注入漏洞、baigo CMS 跨站脚本漏洞（CNVD-2021-53924）”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 4935 个，与上周（4147 个）环比增加 19%。

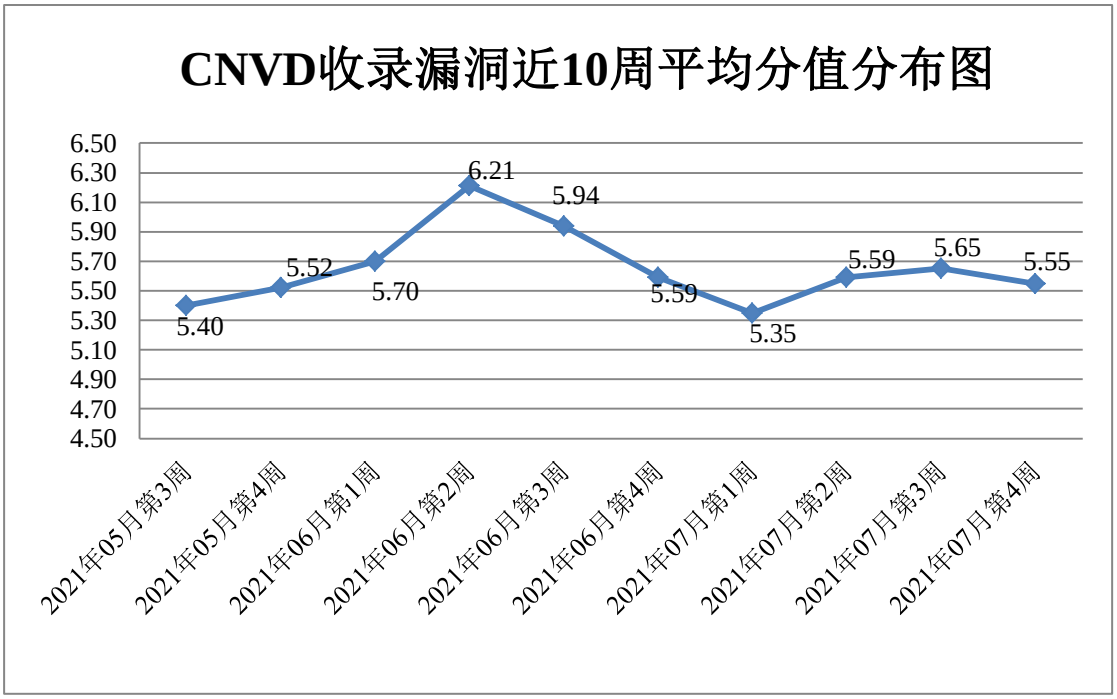

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电

信企业通报漏洞事件 47 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 549 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 41 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 45 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：

紫兴科技集团有限公司、紫光软件系统有限公司、淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、重庆逐越光电科技有限公司、重庆中联信息产业有限责任公司、重庆远秋科技有限公司、中集智能科技有限公司、中国电信集团有限公司、郑州维维信息技术有限公司、浙江大华技术股份有限公司、兄弟（中国）商业有限公司、新浪网技术（中国）有限公司、新道科技股份有限公司、西门子（中国）有限公司、西安华天协同信息技术有限公司、武汉天地伟业科技有限公司、武汉爱码农网络科技有限公司、通用电气（GE）公司、天立泰科技股份有限公司、天地伟业技术有限公司、松下电器（中国）有限公司、四创科技有限公司、数篷科技（深圳）有限公司、曙光信息产业股份有限公司、沈阳明致软件有限公司、深圳市云网万店电子商务有限公司、深圳市迅雷网络技术有限公司、深圳市图美电子技术有限公司、深圳市天地心网络技术有限公司、深圳市群晖智能科技股份有限公司、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、深圳市锟铻科技有限公司、深圳市共济科技股份有限公司、深圳市百为通达科技有限公司、深圳亮钻科技有限公司、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、上海焱凤信息技术有限公司、上海万欣计算机科技有限公司、上海企通数字科技有限公司、上海居亦科技发展有限公司、上海汇尼信息科技有限公司、上海顶想信息科技有限公司、上海步步亿佰科技有限公司、润申信息科技（上海）有限公司、锐捷网络股份有限公司、任子行网络技术股份有限公司、青岛易软天创网络科技有限公司、南通润邦网络科技有限公司、南京易商大路网络科技有限公司、美国菲力尔公司、联想（北京）有限公司、理光（中国）投资有限公司、蓝网科技股份有限公司、聚美优品科技有限公司、飓风（深圳）软件有限公司、锦江区闪灵网络服务部、嘉兴想天信息科技有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南奥科网络技术股份有限公司、湖北大鹏网络科技有限公司、杭州企达信息技术有限公司、杭州巨峰科技有限公司、杭州海康威视数字技术股份有限公司、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、广州易达建信科技开发有限公司、广州市奥威亚电子科技有限公司、广州凯软信息科技有限公司、广州京思顿电子科技有限公司、福州目雪科技有限公司、东莞市通天星软件科技有限公司、成都康菲顿特网络科技有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、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、北京优炫软件股份有限公司、北京学而思教育科技有限

公司、北京星网锐捷网络技术有限公司、北京五一视界数字孪生科技股份有限公司、北京网易有道计算机系统有限公司、北京万维盈创科技发展有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京搜狗信息服务有限公司、北京数科网维技术有限责任公司、北京时空智友科技有限公司、北京时代创信科技有限公司、北京雷霆万钧网络科技有限责任公司、北京金和网络股份有限公司、北京鼎软科技有限公司、北京棣南新宇科技有限公司、北京春笛网络信息技术服务有限公司、北京创新乐知网络技术有限公司、北京辰信领创信息技术有限公司、北京比邻科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、蚌埠依爱消防电子有限责任公司、安美世纪（北京）科技有限公司、安徽渔之蓝教育软件技术有限公司、安徽阳光心健心理咨询有限公司、安徽省科迅教育装备有限公司、爱普生（中国）有限公司、深圳惠通网络、帝国软件、施耐德（Schneider Electric）、万通 CMS、梦想 CMS、华夏 ERP、DocCms X 开发团队、WordPress、VisualSVN Software Ltd.、The Apache Software Foundation、Shirnecms、SEACMS、Oracle、Nagios、maccms、Lexmark、jrkAdmin、jflyfox、Jfinal cms、Irfan Skiljan、HuCart、HongCMS、DzzOffice、Catfish CMS、Axis Communications AB 和 akcms。

本周，CNVD 发布了《Oracle 发布 2021 年 7 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6661

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、北京数字观星科技有限公司、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。山东云天安全技术有限公司、联想全球安全实验室、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、安徽长泰信息安全服务有限公司、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、上海纽盾科技股份有限公司、河南灵创电子科技有限公司、山东新潮信息技术有限公司、北京安帝科技有限公司、北京天地和兴科技有限公司、重庆贝特计算机系统工程有限公司、杭州迪普科技股份有限公司、京东云安全、江西省掌控者信息安全技术有限公司、武汉明嘉信信息安全检测评估有限公司、杭州海康威视数字技术股份有限公司、四川哨兵信息科技有限公司、河南信安世纪科技有限公司、星云博创科技有限公司、广东蓝爵网络安全技术股份有限公司、南京树安信息技术有限公司、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、浙江菜鸟供应链管理有限公司、河南东方云盾信息技术有限公司、江苏保旺达软件技术有限公司、杰润鸿远（北京）科技有限公司、浙江国利网安科技有限公司、浙江木链物联网科技有限公司、北京君云天下科技有限公

司、海南神州希望网路有限公司、四川赛闯检测股份有限公司、北京科技大学、中国工程物理研究院计算机应用研究所、广州安亿信软件科技有限公司、北京机沃科技有限公司、亚信科技（成都）有限公司及其他个人白帽子向 CNVD 提交了 4935 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 2228 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）	1044	1044
北京天融信网络安全技术有限公司	681	22
北京神州绿盟科技有限公司	640	7
奇安信网神（补天平台）	637	637
上海交大	547	547
北京数字观星科技有限公司	279	0
哈尔滨安天科技集团股份有限公司	252	0
华为技术有限公司	204	0
恒安嘉新（北京）科技股份公司	121	0
新华三技术有限公司	86	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）	58	0
浙江大华技术股份有限公司	13	13
北京启明星辰信息安全技术有限公司	11	11
卫士通信息产业股份有限公司	8	37
南京联成科技发展股份有限公司	7	7

中国电信集团系统集成有限责任公司	4	4
北京知道创宇信息技术股份有限公司	3	0
南京铱迅信息技术股份有限公司	2	2
西安四叶草信息技术有限公司	1	1
山东云天安全技术有限公司	581	581
联想全球安全实验室	389	1
北京信联科汇科技有限公司	364	364
北京山石网科信息技术有限公司	171	171
安徽长泰信息安全服务有限公司	88	88
南京众智维信息科技有限公司	72	72
山东泽鹿安全技术有限公司	43	43
上海纽盾科技股份有限公司	30	30
河南灵创电子科技有限公司	30	30
山东新潮信息技术有限公司	24	24
北京安帝科技有限公司	22	22
北京天地和兴科技有限公司	22	22
中国电信股份有限公司网络安全产品运营中心	20	0

重庆贝特计算机系统工程有限公司	16	16
杭州迪普科技股份有限公司	15	1
京东云安全	15	15
江西省掌控者信息安全技术有限公司	14	14
武汉明嘉信信息安全检测评估有限公司	11	11
杭州海康威视数字技术股份有限公司	10	10
四川哨兵信息科技有限公司	8	8
河南信安世纪科技有限公司	8	8
星云博创科技有限公司	7	7
广东蓝爵网络安全技术股份有限公司	5	5
南京树安信息技术有限公司	4	4
贵州多彩宝互联网服务有限公司	4	4
重庆都会信息科技有限公司	4	4
浙江菜鸟供应链管理有限公司	3	3
河南东方云盾信息技术有限公司	3	3
江苏保旺达软件技术有限公司	3	3
杰润鸿远（北京）科技有限公司	3	3
浙江国利网安科技有	2	2

限公司		
浙江木链物联网科技有限公司	2	2
北京君云天下科技有限公司	2	2
海南神州希望网路有限公司	2	2
四川赛闯检测股份有限公司	1	1
北京科技大学	1	1
中国工程物理研究院计算机应用研究所	1	1
广州安亿信软件科技有限公司	1	1
北京机沃科技有限公司	1	1
亚信科技（成都）有限公司	1	1
CNCERT 山东分中心	5	5
CNCERT 四川分中心	1	1
个人	1016	1016
报送总计	7623	4935

本周漏洞按类型和厂商统计

本周，CNVD 收录了 594 个漏洞。WEB 应用 243 个，应用程序 192 个，网络设备（交换机、路由器等网络端设备）51 个，操作系统 40 个，智能设备（物联网终端设备）31 个，数据库 25 个，安全产品 12 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	243
应用程序	192
网络设备（交换机、路由器等网络端设备）	51
操作系统	40
智能设备（物联网终端设备）	31
数据库	25

安全产品	12

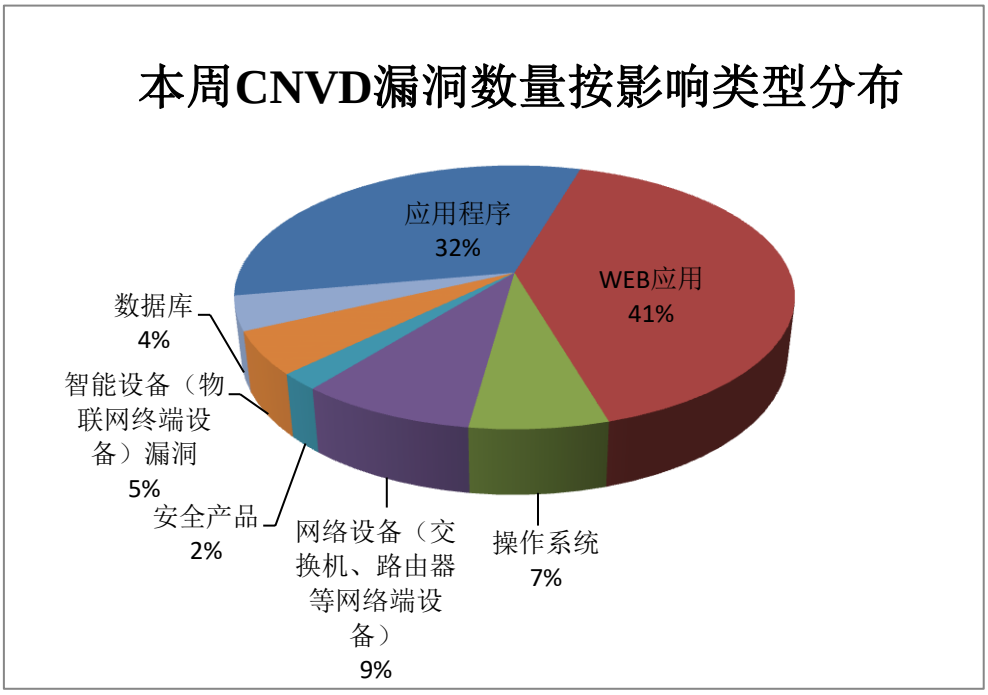

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SIEMENS、NETGEAR、Oracle 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	26	5%
2	NETGEAR	25	4%
3	Oracle	23	4%
4	Google	22	4%
5	Adobe	20	3%
6	武汉爱码农网络科技有限公司	19	3%
7	WordPress	14	2%
8	Nextcloud	12	2%
9	IBM	11	2%
10	其他	422	71%

本周行业漏洞收录情况

本周，CNVD 收录了 35 个电信行业漏洞，36 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Facebook WhatsApp for Android 路径遍历漏洞、D-LINK DIR-3040 信任管理问题漏洞、Google Android System 权限提升漏洞（CNVD-2021

-52344）、多款 Siemens 产品代码问题漏洞”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/

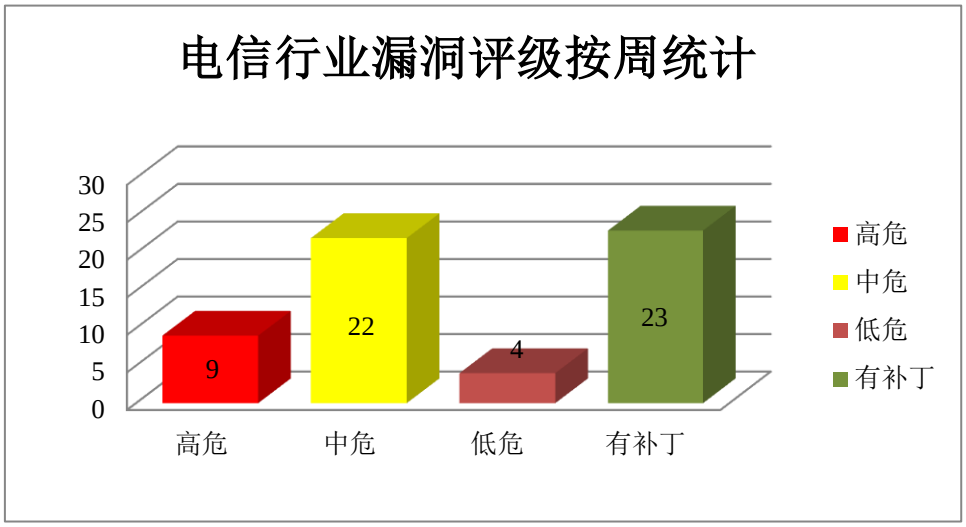

图 3 电信行业漏洞统计

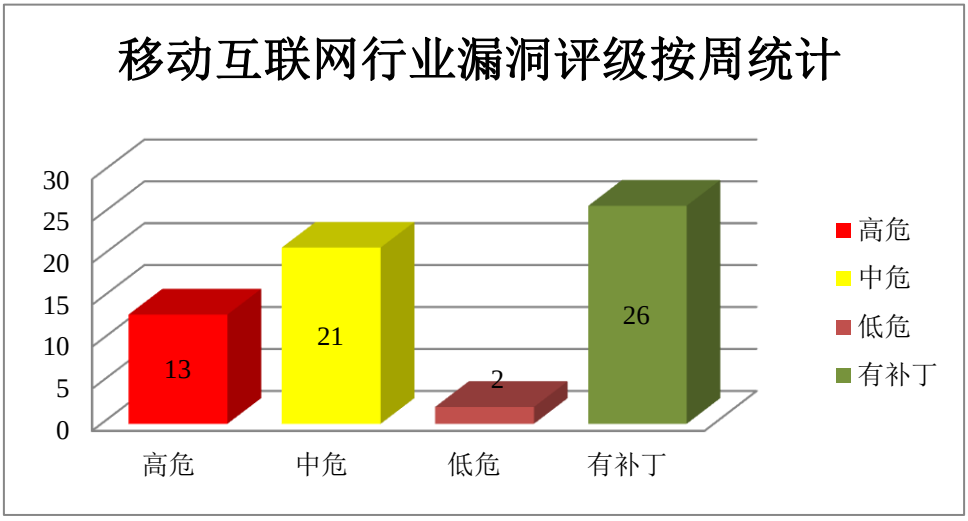

图 4 移动互联网行业漏洞统计

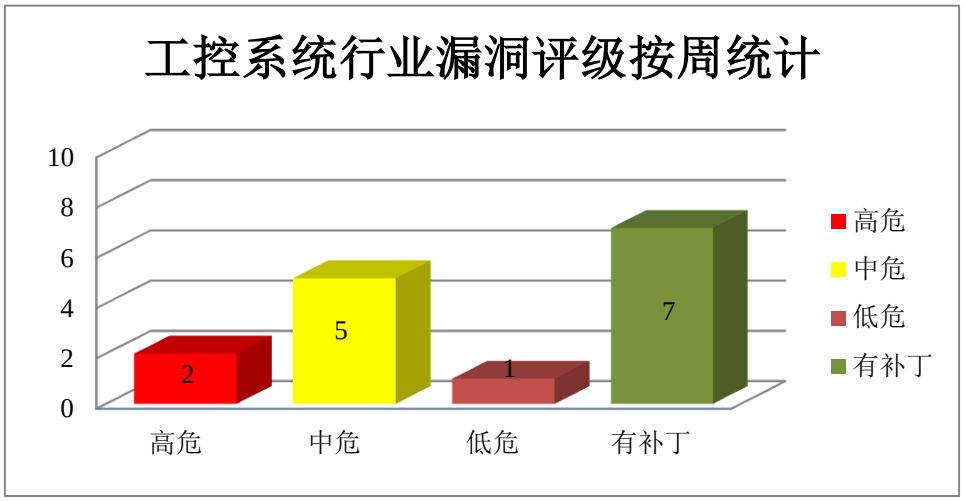

图 5 工控系统行业漏洞统计

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、NETGEAR 产品安全漏洞

NETGEAR R6300 是一款无线路由器。NETGEAR PLW1000 是一款电力线通讯调制解调器。NETGEAR D7800 是一款无线调制解调器。NETGEAR R7500 是一款无线路由器。NETGEAR WNDR3700 和 NETGEAR R6220 都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR R6250 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR EX6200 等都是美国网件（NETGEAR）公司的一款无线网络信号扩展器。NETGEAR WAC510、NETGEAR WAC505 和 NETGEAR WAC510 都是美国网件（NETGEAR）公司的一款无线接入点（AP）。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身份验证，提升权限，执行非法操作系统命令，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：NETGEAR R6300、PLW1000 和 PLW1010 授权问题漏洞、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-52563）、多款 NETGEAR 产品跨站请求伪造漏洞（CNVD-2021-52569）、NETGEAR WNDR3700 和 R6220 操作系统命令注入漏洞、NETGEAR WAC510 授权问题漏洞、NETGEAR WAC510 权限提升漏洞、NETGEAR WAC505 和 WAC510 操作系统命令注入漏洞、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-52952）。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-2021-52565

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52563

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52569

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52567

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52946

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52945

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52947

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52952

2、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在远程代码执行和权限提升漏洞，攻击者可利用漏洞导致本地权限提升，实现远程代码执行。

CNVD 收录的相关漏洞包括：Google Android System 远程代码执行漏洞（CNVD-2021-52330、CNVD-2021-52331）、Google Android System 权限提升漏洞（CNVD-2021-52340、CNVD-2021-52338、CNVD-2021-52343、CNVD-2021-52341、CNVD-2021-52344）、Google Android Media Framework 权限提升漏洞（CNVD-2021-52346）。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-2021-52330

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52331

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52340

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52338

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52343

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52341

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52346

https://www.cnvd.org.cn/flaw/show/CNVD-2021-52344

3、Adobe 产品安全漏洞

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。Adobe Premiere Pro 是 Adobe 公司推出的一款基于时间轴的视频编辑软件。Adobe Prelude 是一款专为媒体整理和元数据输入而设计的视频记录和采集工具，可快速标记和转码视频素材并快速创建粗剪。Adobe Character Animator 是一款动作捕获和动画制作工具,它可以为每个人提供一个用于直观地制作 2D 人物动画、实时动画以及轻松共享和发布人物的易于使用的解决方案。Adobe After Effects（简称“AE”）是 Adobe 公司推出的一款图形视频处理软件，适用于从事设计和视频特技的机构，包括电视台、动画制作公司、个人后期制作工作室以及多媒体工作室。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。

CNVD 收录的相关漏洞包括：Adobe Photoshop 栈缓冲区溢出漏洞、Adobe Premiere Pro 内存越界访问漏洞、Adobe Prelude 内存越界访问漏洞、Adobe Character Animator 内存越界访问漏洞、Adobe After Effects 越界写入漏洞（CNVD-2021-54342、CNVD

-2021-54341）、Adobe After Effects 内存越界访问漏洞（CNVD-2021-54339、CNVD-2021-54343）。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-2021-54332
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54338
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54336
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54334
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54342
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54341
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54339
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54343

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拒绝服务漏洞，攻击者可利用漏洞导致拒绝服务。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2021-54025、CNVD-2021-54027、CNVD-2021-54369、CNVD-2021-54368、CNVD-2021-54372、CNVD-2021-54371、CNVD-2021-54370、CNVD-2021-54375）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-2021-54025
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54027
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54369
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54368
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54372
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54371
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54370
https://www.cnvd.org.cn/flaw/show/CNVD-2021-54375

5、D-LINK DIR-3040 信息泄露漏洞（CNVD-2021-53338）

D-LINK DIR-3040 是中国台湾友讯（D-Link）公司的一个路由器，提供连接网络的功能。本周，D-LINK DIR-3040 被披露存在信息泄露漏洞。攻击者可利用该漏洞发送 HTTP 请求导致敏感信息的泄露。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-2021-53338

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-2021-51793	IBM Security Access Manager 信息泄露漏洞（CNVD-2021-51793）	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.ibm.com/support/pages/node/6471903
CNVD-2021-51805	MetInfo SQL 注入漏洞（CNVD-2021-51805）	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.mituo.cn/news/2473.html
CNVD-2021-52409	Fluent Bit 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://oss-fuzz.com/revisions?job=honggfuzz_asan_fluent-bit&range=202105060607:202105070621。
CNVD-2021-53330	Redis 远程代码执行漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://redislabs.com/
CNVD-2021-53342	PostgreSQL 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://bugzilla.redhat.com/show_bug.cgi?id=1954112
CNVD-2021-53901	Facebook WhatsApp for Android 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://www.whatsapp.com/security/advisories/2021/
CNVD-2021-53908	ZOHO ManageEngine ServiceDesk Plus 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，补丁获取链接：https://www.tenable.com/security/research/tra-2021-22
CNVD-2021-53919	EIPStackGroup OpENer EtherNet/IP 拒绝服务漏洞	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://github.com/EIPStackGroup/OpENer
CNVD-2021-54360	多款 SIMATIC 软件产品远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-599968.pdf
CNVD-2021-54395	Linux kernel 缓冲区溢出漏洞（CNVD-2021-54395）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://ubuntu.com/security/CVE-2021-3490

小结：本周，NETGEAR 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，提升权限，执行非法操作系统命令，导致缓冲区溢出或堆溢出等。此外，Google、Adobe、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升，执行任意代码，导致拒绝服务。另外，D-LINK DIR-3040 被披露存在信息泄露漏洞。攻击者可利用该漏洞发送 HTTP 请求导致敏感信息的泄露。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、LJCMS SQL 注入漏洞

验证描述

LJCMS 是一款自由和开放源码的内容管理系统。

LJCMS 存在 SQL 注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。

验证信息

POC 链接：https://github.com/Q1ngShan/PHP_Learning/issues/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-53923

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. 微软新漏洞 PetitPotam：允许攻击者获取 Windows 系统的哈希密码

一名研究人员 Windows 操作系统中发现了一个漏洞，命名为 PetitPotam。攻击者可利用该漏洞强制远程 Windows 机器共享其哈希密码。

参考链接：https://securityaffairs.co/wordpress/120489/hacking/windows-petitpotam-attack.html

2. Linux 内核中的 LPE 漏洞允许攻击者获得大多数发行版的 root 权限

Qualys 研究人员发现了一个本地权限提升漏洞（LPE），其编号为 CVE-2021-33909，又名 Sequoia，无特权的攻击者可以利用该漏洞在大多数 Linux 发行版上获得 root 权限。

参考链接：https://securityaffairs.co/wordpress/120365/security/lpe-flaw-linux-kernel.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