

信息安全漏洞周报

2022年01月24日-2022年02月06日

2022年第4、5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 721 个，其中高危漏洞 190 个、中危漏洞 450 个、低危漏洞 81 个。漏洞平均分为 5.59。本周收录的漏洞中，涉及 0day 漏洞 307 个（占 43%），其中互联网上出现“pimcore 跨站脚本漏洞(CNVD-2022-07500)、Blackmagic Design DaVinci Resolve 代码执行漏洞”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 6178 个，与上周（5941 个）环比增加 4%。

CNVD收录漏洞近10周平均分分布图

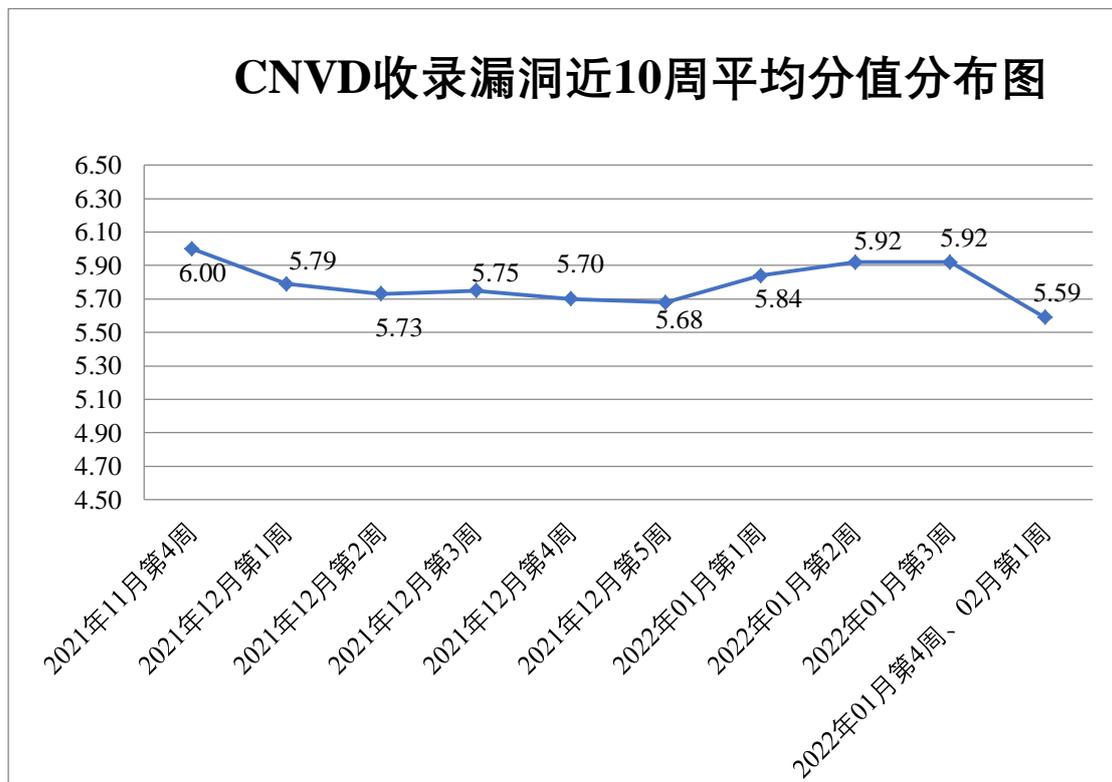


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 33 起，向基础电信企业通报漏洞事件 32 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 717 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 137 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 182 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：

江西铭软科技有限公司、深圳勤杰软件有限公司、杭州飞致云信息科技有限公司、北京国测星绘信息技术有限公司、芜湖市广电传媒（集团）有限公司、厦门四信通信科技有限公司、北京超图软件股份有限公司、成都生动网络科技有限公司、小米科技有限责任公司、成都点威科技有限公司、华硕电脑（上海）有限公司、山东力创科技股份有限公司、北京神州泰岳软件股份有限公司、统信软件技术有限公司、西安众邦网络科技有限公司、微软（中国）有限公司、中煤（西安）地下空间科技发展有限公司、兄弟（中国）商业有限公司、安徽省科迅教育装备有限公司、北京棣南新宇科技有限公司、北京致远互联软件股份有限公司、长沙友点软件科技有限公司、深圳市吉祥腾达科技有限公司、北京汉邦高科数字技术股份有限公司、西安艾润物联网技术服务有限责任公司、广东东宏智控科技股份有限公司、新天科技股份有限公司、普联技术有限公司、上海汉得信息技术股份有限公司、北京星网锐捷网络技术有限公司、众勤通信设备贸易（上海）有限公司、成都飞鱼星科技股份有限公司、联奕科技股份有限公司、傲拓科技股份有限公司、安徽东位信息科技有限公司、广州红海云计算股份有限公司、成都万江港利科技有限公司、苏州科达科技股份有限公司、畅捷通信息技术股份有限公司、网宿科技股份有限公司、惠普贸易（上海）有限公司、松下电器（中国）有限公司、上海泛微网络科技有限公司、友讯电子设备（上海）有限公司、广州市高科通信技术股份有限公司、拓尔思信息技术股份有限公司、上海瑞美信息技术有限公司、上海二三四五移动科技有限公司、广联达科技股份有限公司、浙江智游宝信息科技有限公司、大庆紫金桥软件技术有限公司、迈普通信技术股份有限公司、北京中广上洋科技股份有限公司、杭州海康威视数字技术股份有限公司、湖北点点点科技有限公司、宁波市科技园区明天医网科技有限公司、天信仪表集团有限公司、北京瑞星网安技术股份有限公司、南京音墙信息技术有限公司、深圳华磊物流通信息科技有限公司、阿里巴巴集团安全应急响应中心、深圳市为爱普信息技术有限公司、北京米尔伟业科技有限公司、广州飞硕信息科技股份有限公司、蚌埠依爱消防电子有限责任公司、北京九思协同软件有限公司、上海英斯泊物联网有限公司、上海纵之格科技有限公司、深圳市迅捷通信技术有限公司、广州红帆科技有限公司、上海企望信息科技有限公司、浙江宇视科技有限公司、哈尔滨新中新电子股份有限公司、深圳市迅雷网络技术有限公司、山东山大华天软件有限公司、浙江大华

技术股份有限公司、海南赞赞网络科技有限公司、中电鸿信信息科技有限公司、吉翁电子（深圳）有限公司、杭州商易信息技术有限公司、深圳市思迅软件股份有限公司、新秀工作室、西安智尼链电子科技有限公司、上海贝锐信息科技股份有限公司、北京猎鹰安全科技有限公司、北京安迪盛安全系统自动化有限公司、湖南青果软件有限公司、亚信科技（成都）有限公司、腾讯安全应急响应中心、长沙米拓信息技术有限公司、海南省吉胜网络信息科技有限公司、润申信息科技（上海）有限公司、深圳市博思协创网络科技有限公司、上海博达数据通信有限公司、北京谋智火狐信息技术有限公司、淄博闪灵网络科技有限公司、青岛东胜伟业软件有限公司、东方财富安全应急响应中心、北京通达信科科技有限公司、东莞市光速网络技术有限公司、上海赛连信息科技有限公司、北京华富远科技有限公司、HuCart、PHPEMSMuYuCMS、Sapido Technology Inc、taoCMS、Hutool、Axis Communications AB、Cockroach Labs、Espruino、DataGear、ArrayNetworks、PhpaaCMS、Gin-View-admin、Adobe、Moddable、MOBOTIX、The Apache Software Foundation、SEMCMS、ZZCMS。

本周，CNVD 发布了《Oracle 发布 2022 年 1 月的安全公告》。详情参见 CNVD 网站公告内容。

<https://www.cnvd.org.cn/webinfo/show/7336>

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、杭州安恒信息技术股份有限公司、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、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、山东云天安全技术有限公司、北京华云安信息技术有限公司、南京树安信息技术有限公司、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、北京山石网科信息技术有限公司、福建省海峡信息技术有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、上海纽盾科技股份有限公司、广西等保安全测评有限公司、思而听网络科技有限公司、河南信安世纪科技有限公司、贵州多彩宝互联网服务有限公司、博智安全科技股份有限公司、北京远禾科技有限公司、中通服和信科技有限公司、深圳昂楷科技有限公司、有度网络安全技术有限公司、重庆都会信息科技有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、中国工商银行、北京威努特技术有限公司、北京机沃科技有限公司、南京领行科技股份有限公司及其他个人白帽子向 CNVD 提交了 4942 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 2377 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
上海交大	1138	1138
奇安信网神（补天平台）	926	926
斗象科技（漏洞盒子）	313	313
新华三技术有限公司	264	0
杭州安恒信息技术股份有限公司	232	133
北京天融信网络安全技术有限公司	137	23
恒安嘉新（北京）科技股份有限公司	132	0
安天科技集团股份有限公司	126	0
北京数字观星科技有限公司	72	0
北京启明星辰信息安全技术有限公司	62	0
天津市国瑞数码安全系统股份有限公司	59	0
西安四叶草信息技术有限公司	50	50
远江盛邦（北京）网络安全科技股份有限公司	27	27
中国电信集团系统集成有限责任公司	17	1
京东科技信息技术有限公司	8	8
北京神州绿盟科技有限公司	8	8
深信服科技股份有限公司	8	6
北京长亭科技有限公司	4	4

北京智游网安科技有限公司	1	1
内蒙古云科数据服务股份有限公司	1	1
北京知道创宇信息技术股份有限公司	1	0
北京华顺信安科技有限公司	252	1
山东云天安全技术有限公司	160	160
北京华云安信息技术有限公司	139	139
南京树安信息技术有限公司	92	92
广东蓝爵网络安全技术股份有限公司	86	86
杭州海康威视数字技术股份有限公司	55	55
北京山石网科信息技术有限公司	30	30
福建省海峡信息技术有限公司	29	29
亚信科技（成都）有限公司	23	0
山东新潮信息技术有限公司	23	23
河南灵创电子科技有限公司	17	17
杭州迪普科技股份有限公司	15	0
内蒙古洞明科技有限公司	12	12
上海纽盾科技股份有限公司	10	10
广西等保安全测评有	8	8

限公司		
思而听网络科技有限公司	6	6
河南信安世纪科技有限公司	5	5
贵州多彩宝互联网服务有限公司	4	4
博智安全科技股份有限公司	4	4
北京远禾科技有限公司	3	3
中通服和信科技有限公司	3	3
深圳昂楷科技有限公司	2	2
有度网络安全技术有限公司	2	2
重庆都会信息科技有限公司	2	2
河南东方云盾信息技术有限公司	2	2
快页信息技术有限公司	1	1
中国工商银行	1	1
北京威努特技术有限公司	1	1
北京机沃科技有限公司	1	1
南京领行科技股份有限公司	1	1
个人	1603	1603
报送总计	6178	4942

本周，CNVD 收录了 721 个漏洞。WEB 应用 295 个，应用程序 250 个，网络设备（交换机、路由器等网络端设备）67 个，操作系统 41 个，智能设备（物联网终端设备）33 个，数据库 20 个，安全产品 15 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	295
应用程序	250
网络设备（交换机、路由器等网络端设备）	67
操作系统	41
智能设备（物联网终端设备）	33
数据库	20
安全产品	15

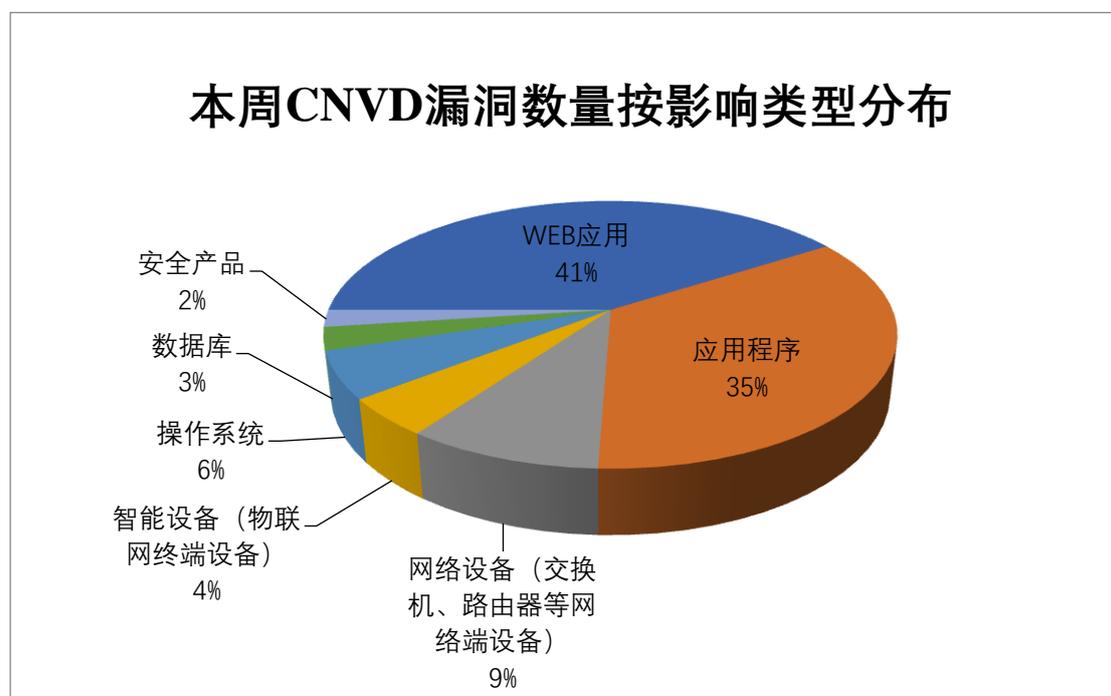


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及淄博闪灵网络科技有限公司、JerryScript、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	淄博闪灵网络科技有限公司	28	4%
2	JerryScript	22	3%
3	NETGEAR	20	3%
4	Oracle	19	3%
5	WordPress	19	2%

6	GPAC	16	2%
7	Huawei	15	2%
8	Pimcore	14	2%
9	Google	14	2%
10	其他	554	77%

本周行业漏洞收录情况

本周，CNVD 收录了 42 个电信行业漏洞，18 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-2640 路径遍历漏洞、NETGEAR R6400 v2 缓冲区溢出漏洞”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/>

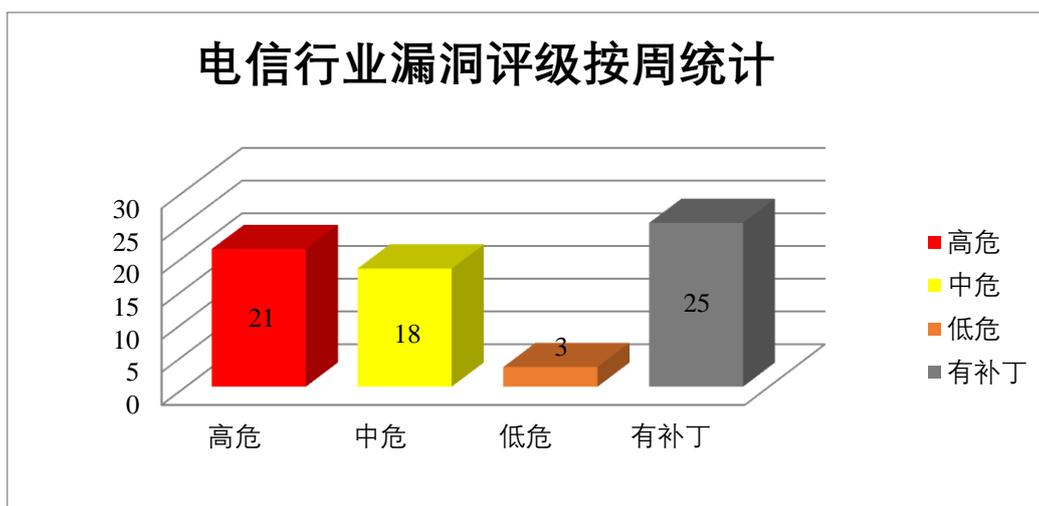


图 3 电信行业漏洞统计

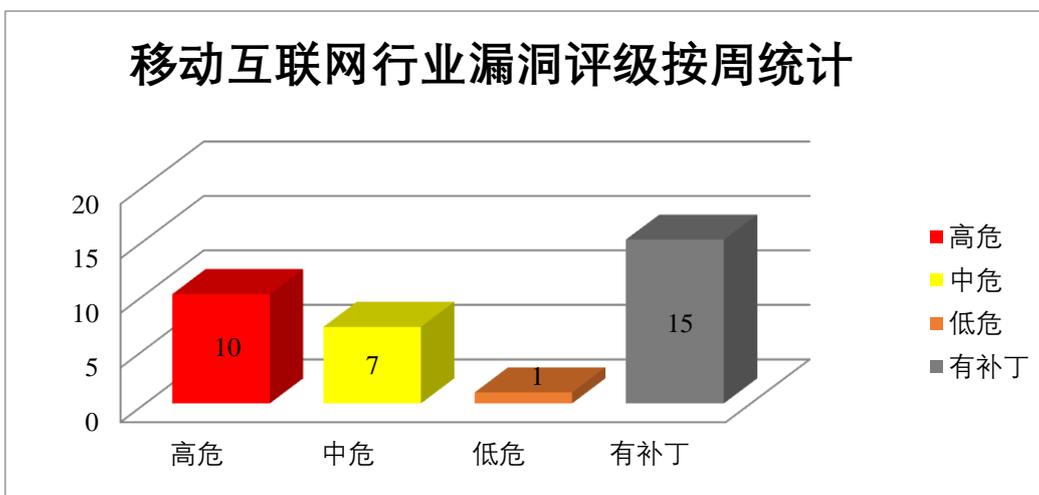


图 4 移动互联网行业漏洞统计

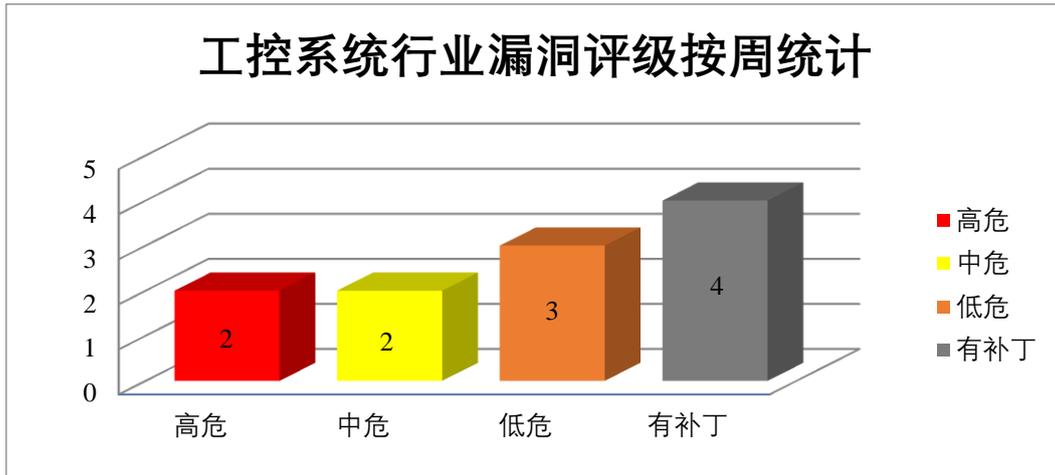


图 5 工控系统行业漏洞统计

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 Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞导致缓冲区溢出，整数溢出，提升权限等。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2022-06153）、Google Android 输入验证错误漏洞（CNVD-2022-06152）、Google Android 越界写入漏洞（CNVD-2022-06154、CNVD-2022-06897）、Google Android 权限提升漏洞（CNVD-2022-06157、CNVD-2022-06156、CNVD-2022-06158）、Google Android 逻辑缺陷漏洞。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-2022-06153>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06152>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06154>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06157>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06156>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06158>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06899>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06897>

2、Cisco 产品安全漏洞

Cisco Security Manager（CSM）是美国思科（Cisco）公司的一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙。VPN 和入侵保护安全服务。本

周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞对该界面的用户进行跨站点脚本攻击，导致代码执行，信息泄漏等。

CNVD 收录的相关漏洞包括：Cisco Security Manager 跨站脚本漏洞（CNVD-2022-06378、CNVD-2022-06377、CNVD-2022-06380、CNVD-2022-06379、CNVD-2022-06383、CNVD-2022-06382、CNVD-2022-06381、CNVD-2022-06386）。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-2022-06378>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06377>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06380>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06379>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06383>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06382>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06381>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06386>

3、NETGEAR 产品安全漏洞

NETGEAR D7000 是美国网件（Netgear）公司的一款无线调制解调器。NETGEAR xr1000 是美国网件（Netgear）公司的一款路由器。NETGEAR R6700v2 是美国网件（Netgear）公司的一款无线路由器。NETGEAR R8000 是美国网件（Netgear）公司的一款无线路由器。NETGEAR R6260 是美国网件（Netgear）公司的一款路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞绕过访问控制，造成拒绝服务攻击，在 root 上下文中执行代码等。

CNVD 收录的相关漏洞包括：Netgear NETGEAR D7000 授权问题漏洞（CNVD-2022-06684、CNVD-2022-06687）、NETGEAR D7000 和 NETGEAR 授权问题漏洞、NETGEAR XR1000 信任管理问题漏洞、NETGEAR R6700v2 权限许可和访问控制问题漏洞、NETGEAR R8000 缓冲区溢出漏洞（CNVD-2022-06691）、NETGEAR R6260 堆栈的缓冲区溢出漏洞、NETGEAR R6260 mini_httpd SOAP 缓冲区溢出漏洞。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-2022-06684>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06687>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06685>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06688>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06692>
<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06691>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06695>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-06694>

4、Oracle 产品安全漏洞

Oracle MySQL Cluster 是美国甲骨文（Oracle）公司开发的一个写可扩展、实时。兼容 ACID 的事务型数据库。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞破坏或删除数据，执行任意代码等。

CNVD 收录的相关漏洞包括：Oracle MySQL Cluster 输入验证错误漏洞（CNVD-2022-07913、CNVD-2022-07912、CNVD-2022-07915、CNVD-2022-07914、CNVD-2022-07919、CNVD-2022-07923、CNVD-2022-07926、CNVD-2022-07925）。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-2022-07913>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07912>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07915>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07914>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07919>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07923>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07926>

<https://www.cnvd.org.cn/flaw/show/CNVD-2022-07925>

5、Moddable SDK 拒绝服务漏洞

Moddable SDK 是美国 Moddable 公司的一套用于物联网嵌入式软件开发的软件开发工具包（SDK）。本周，Moddable SDK 被披露存在拒绝服务漏洞。攻击者可利用该漏洞导致拒绝服务。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-2022-08217>

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-2022-06151	Google Android 输入验证错误漏洞（CNVD-2022-06151）	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://source.android.com/security/bulletin/pixel/2022-01-01
CNVD-2022-06481	OnionShare 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/onionshare/onions

			hare/compare/v2.3.3...v2.4
CNVD-2022-06494	Western Digital My Cloud OS 5 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.westerndigital.com/support/product-security/wdc-22002-my-cloud-os5-firmware-5-19-117
CNVD-2022-06504	WordPress 插件 uListing 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://patchstack.com/database/vulnerability/ulisting/wordpress-ulisting-plugin-2-0-5-unauthenticated-privilege-escalation-vulnerability
CNVD-2022-06535	ReadyMedia 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://sourceforge.net/projects/minidlna/files/latest/download
CNVD-2022-06539	PostgreSQL 任意代码执行漏洞（CNVD-2022-06539）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.postgresql.org/about/news/postgresql-131-125-1110-1015-9620-and-9524-released-2111/
CNVD-2022-06540	SPIP 参数验证不当漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://git.spip.net/spip/spip/commit/a4267eba1022dabc12831ddb021c5d6e09040f8
CNVD-2022-06547	InfluxDB 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://github.com/influxdata/influxdb/commit/761b557315ff9c1642cf3b0e5797cd3d983a24c0
CNVD-2022-06550	HorizontCMS 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/ttimot24/HorizontCMS/commit/d47ac683791a238f7d1462058d5169800fa35025
CNVD-2022-06682	Juniper Networks Junos OS 拒绝服务漏洞（CNVD-2022-06682）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11286

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用该漏洞导致缓冲区溢出，整数溢出，提升权限等。此外，Cisco、NETGEAR、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞破坏或删除数据，导致代码执行，信息泄漏等。另外，

Moddable SDK 被披露存在拒绝服务漏洞。攻击者可利用该漏洞导致拒绝服务。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、Blackmagic Design DaVinci Resolve 代码执行漏洞

验证描述

Blackmagic Design DaVinci Resolve 是一款将剪辑、色彩校正、视觉效果、动态图形和音频后期制作集于一身的软件工具。

Blackmagic Design DaVinci Resolve 存在代码执行漏洞，攻击者可利用该漏洞在应用程序上下文中执行任意代码。

验证信息

POC 链接: https://talosintelligence.com/vulnerability_reports/TALOS-2021-1427

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2022-06884>

信息提供者

恒安嘉新(北京)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. Linux 系统爆出新漏洞，扎根在所有的发行版本中

近日，网络安全研究人员发布消息称，Polkit 的 pkexec 组件中存在一个安全漏洞（CVE-2021-4034），这意味着几乎所有的 Linux 发行版的默认配置都包含此漏洞，攻击者可通过该漏洞获得系统的 root 权限。

参考链接: <https://www.bleepingcomputer.com/news/security/linux-system-service-bug-gives-root-on-all-major-distros-exploit-released/>

2. 微软分享针对 Mac 的 UpdateAgent 复杂木马的细节

微软与苹果合作修补 macOS 设备中的“Shrootless”漏洞，微软已经提供了有关一个针对 Mac 的复杂木马的详细信息。

参考链接: <https://www.cnbeta.com/articles/tech/1232927.htm>

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