国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 02 月 28 日-2022 年 03 月 06 日 **2022 年第 9 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 569 个，其中高危漏洞 160 个、中危漏洞 373 个、低危漏洞 36 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 298 个（占 52%），其中互联网上出现“WordPress 插件 Survey & Poll SQL 注入漏洞、WordPress 插件 WP Guppy 敏感信息泄露漏洞”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 4175 个，与上周（5012 个）环比减少 17%。

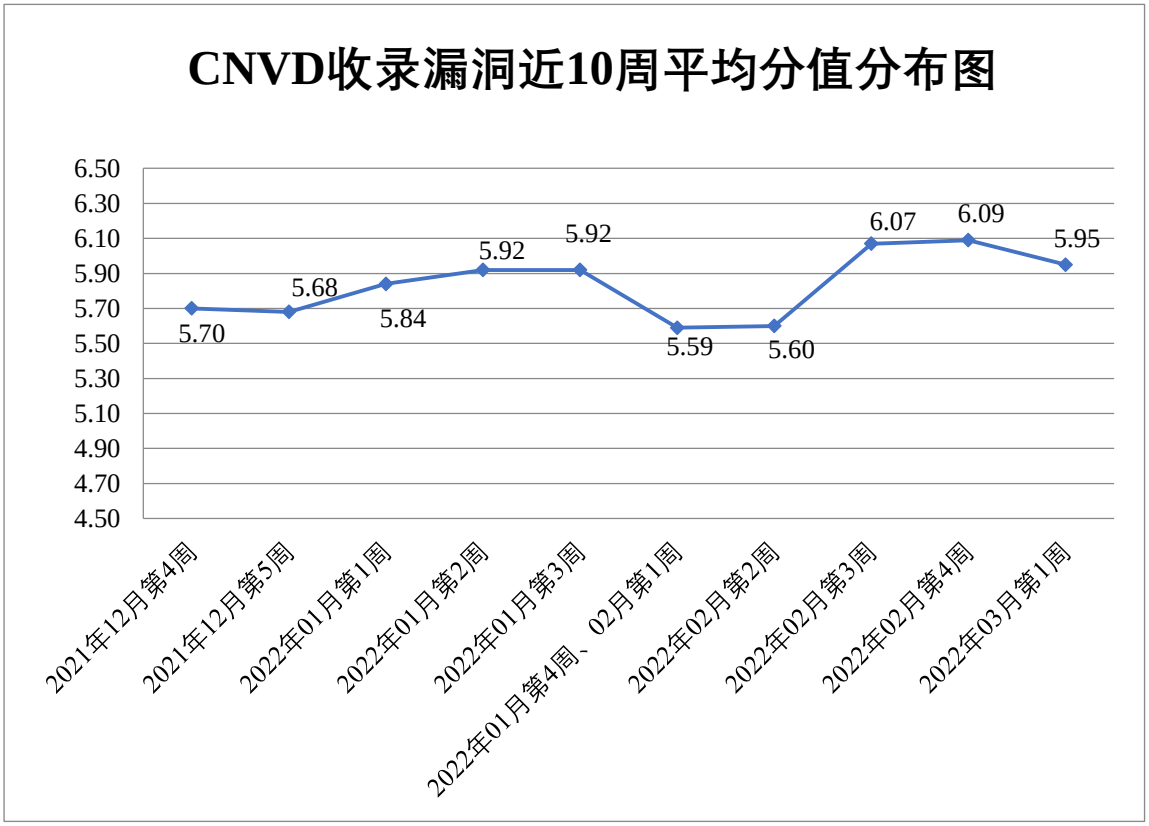

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 23 起，向基础电信企业通报漏洞事件 29 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 694 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 77 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 81 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、珠海新华通软件股份有限公司、珠海市魅族通讯设备有限公司、重庆中联信息产业有限责任公司、重庆森鑫炬科技有限公司、中文在线数字出版集团股份有限公司、中山市同创科技发展有限公司、中科网威信息技术有限公司、中科博华信息科技有限公司、中国船舶重工集团国际工程有限公司、中创软件商用中间件股份有限公司、浙江橙树网络技术有限公司、长沙友点软件科技有限公司、漳州豆壳网络科技有限公司、云从科技集团股份有限公司、友讯电子设备（上海）有限公司、永中软件股份有限公司、亚太卫星宽带通信（深圳）有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、暇光软件科技（上海）有限公司、西安新软信息科技有限公司、武汉神州数码云科网络技术有限公司、武汉达梦数据库股份有限公司、温州互引信息技术有限公司、微软（中国）有限公司、网易公司、天津神州浩天科技有限公司、唐山平升电子技术开发有限公司、索尼（中国）有限公司、苏州科达科技股份有限公司、四创科技有限公司、世邦通信股份有限公司、盛威时代科技集团有限公司、深圳市西迪特科技有限公司、深圳市万网博通科技有限公司、深圳市图美电子技术有限公司、深圳市思迅软件股份有限公司、深圳市锟铻科技有限公司、深圳市吉祥腾达科技有限公司、深圳市大疆创新科技有限公司、深圳市必联电子有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海依图网络科技有限公司、上海天旦网络科技发展有限公司、上海脉信网络科技有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、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、上海贝锐信息科技股份有限公司、上海艾泰科技有限公司、山脉科技股份有限公司、山东中创软件商用中间件股份有限公司、厦门四信通信科技有限公司、厦门才茂通信科技有限公司、三星（中国）投资有限公司、青岛聚城网络科技有限公司、南宁旭东网络科技有限公司、柯尼卡美能达（中国）投资有限公司、江西铭软科技有限公司、佳能（中国）有限公司、华平信息技术股份有限公司、河北南昊高新技术开发有限公司、杭州恩软信息技术有限公司、汉王科技股份有限公司、广州市保伦电子有限公司、广州合优网络科技有限公司、富士施乐(中国)有限公司、福州网钛软件科技有限公司、东芝（中国）有限公司、东软教育科技有限公司、大唐电信科技股份公司、成都星锐蓝海网络科技有限公

司、成都索贝数码科技股份有限公司、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、贝尔金国际有限公司、北京中创视讯科技有限公司、北京云泽晶企数字技术有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京信安世纪科技有限公司、北京人大金仓信息技术股份有限公司、北京旷视科技有限公司、北京金万维科技有限公司、北京超星数图信息技术有限公司、北京百卓网络技术有限公司、安科瑞电气股份有限公司、安徽晶奇网络科技股份有限公司、POLYCOM 通讯技术（北京）有限公司、合优网络、百家 cms、站帮主 CMS、ZbzCMS、Yearning、Yamaha Corporation、UCMS、TuziCMS、Realtek Semiconductor Corporation、phpaaCMS、Netis Systems Co.、Jpress、Iceni Technology Limited、GTEN America N.A. Inc.、DEVA Broadcast Ltd.、BEESCMS、Arista Networks、Adobe 和 ABB。

本周，CNVD 发布了《关于 CNVD 技术组支撑单位年度工作情况的公告》、《国家信息安全漏洞共享平台 2021 年工作会议成功召开》、《关于南京众智维等 10 家单位具备 CNVD 支撑单位资格的公告》、《CNVD 原创漏洞积分激励机制（第三版）》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7436

https://www.cnvd.org.cn/webinfo/show/7441

https://www.cnvd.org.cn/webinfo/show/7451

https://www.cnvd.org.cn/webinfo/show/7446

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、安天科技集团股份有限公司、西安四叶草信息技术有限公司、阿里云计算有限公司、北京神州绿盟科技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、杭州默安科技有限公司、重庆都会信息科技有限公司、贵州多彩宝互联网服务有限公司、泽鹿安全、长春嘉诚信息技术股份有限公司、内蒙古洞明科技有限公司、南京禾盾信息科技有限公司、苏州棱镜七彩信息科技有限公司、快页信息技术有限公司、南京树安信息技术有限公司、武汉安域信息安全技术有限公司、北京华云安信息技术有限公司、华鲁数智信息技术（北京）有限公司、北京山石网科信息技术有限公司、山东新潮信息技术有限公司、深圳建安润星安全技术有限公司、北京远禾科技有限公司、开元华创科技集团、国网山东省电力公司、上海纽盾科技股份有限公司、交通运输信息安全中心有限公司、上海上讯信息技术股份有限公司、杭州海康威视数字技术股份有限公司、河南天祺信息安全技术有限公司、广东蓝爵网络安全技术股份有限公司、河南灵创电子科技有限公司、河南信安世纪科技有限公司、中通服和信科技有限公司、成都智安民扬网络有限公司、安知攻防实验室、博智安全科技股份有限公司、贵州泰若数字科技有限公司、河南东方云盾信息技

术有限公司、上海市信息安全测评认证中心、山石网科通信技术股份有限公司、广西等保安全测评有限公司、天津启明星辰信息技术有限公司及其他个人白帽子向 CNVD 提交了 4175 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 1859 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
斗象科技（漏洞盒子）	675	675
上海交大	658	658
奇安信网神（补天平台）	526	526
新华三技术有限公司	328	0
安天科技集团股份有限公司	208	0
西安四叶草信息技术有限公司	142	142
阿里云计算有限公司	133	0
北京神州绿盟科技有限公司	126	16
恒安嘉新（北京）科技股份公司	123	0
北京启明星辰信息安全技术有限公司	116	61
杭州安恒信息技术股份有限公司	90	30
深信服科技股份有限公司	64	1
北京数字观星科技有限公司	61	0
天津市国瑞数码安全系统股份有限公司	59	0
南京众智维信息科技有限公司	51	51
内蒙古云科数据服务股份有限公司	50	50
中国电信集团系统集	28	0

成有限责任公司		
京东科技信息技术有限公司	27	27
三六零数字安全科技集团有限公司	20	0
北京天融信网络安全技术有限公司	18	18
北京知道创宇信息技术有限公司	5	5
北京安信天行科技有限公司	2	2
北京智游网安科技有限公司	1	1
山东云天安全技术有限公司	143	143
北京华顺信安科技有限公司	125	0
亚信科技（成都）有限公司	59	0
杭州默安科技有限公司	58	58
重庆都会信息科技有限公司	29	29
贵州多彩宝互联网服务有限公司	28	28
泽鹿安全	26	26
长春嘉诚信息技术股份有限公司	25	25
内蒙古洞明科技有限公司	21	21
南京禾盾信息科技有限公司	18	18
苏州棱镜七彩信息科技有限公司	18	18
杭州迪普科技股份有	15	0

限公司		
快页信息技术有限公司	15	15
南京树安信息技术有限公司	14	14
武汉安域信息安全技术有限公司	14	14
北京华云安信息技术有限公司	12	12
华鲁数智信息技术（北京）有限公司	10	10
北京山石网科信息技术有限公司	9	9
山东新潮信息技术有限公司	9	9
深圳建安润星安全技术有限公司	8	8
北京远禾科技有限公司	7	7
开元华创科技集团	5	5
国网山东省电力公司	5	5
上海纽盾科技股份有限公司	5	5
交通运输信息安全中心有限公司	4	4
上海上讯信息技术股份有限公司	4	4
杭州海康威视数字技术股份有限公司	4	4
河南天祺信息安全技术有限公司	2	2
广东蓝爵网络安全技术股份有限公司	2	2
河南灵创电子科技有限公司	2	2

河南信安世纪科技有限公司	2	2
中通服和信科技有限公司	1	1
成都智安民扬网络有限公司	1	1
安知攻防实验室	1	1
博智安全科技股份有限公司	1	1
贵州泰若数字科技有限公司	1	1
河南东方云盾信息技术有限公司	1	1
上海市信息安全测评认证中心	1	1
山石网科通信技术股份有限公司	1	1
广西等保安全测评有限公司	1	1
天津启明星辰信息技术有限公司	1	1
CNCERT 贵州分中心	3	3
CNCERT 宁夏分中心	1	1
CNCERT 四川分中心	1	1
个人	1398	1398
报送总计	5622	4175

本周漏洞按类型和厂商统计

本周，CNVD 收录了 569 个漏洞。应用程序 253 个，WEB 应用 183 个，网络设备（交换机、路由器等网络端设备）64 个，操作系统 30 个，智能设备（物联网终端设备）27 个，安全产品 10 个，数据库 2 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	253
WEB 应用	183

网络设备（交换机、路由器等网络端设备）	64
操作系统	30
智能设备（物联网终端设备）	27
安全产品	10
数据库	2

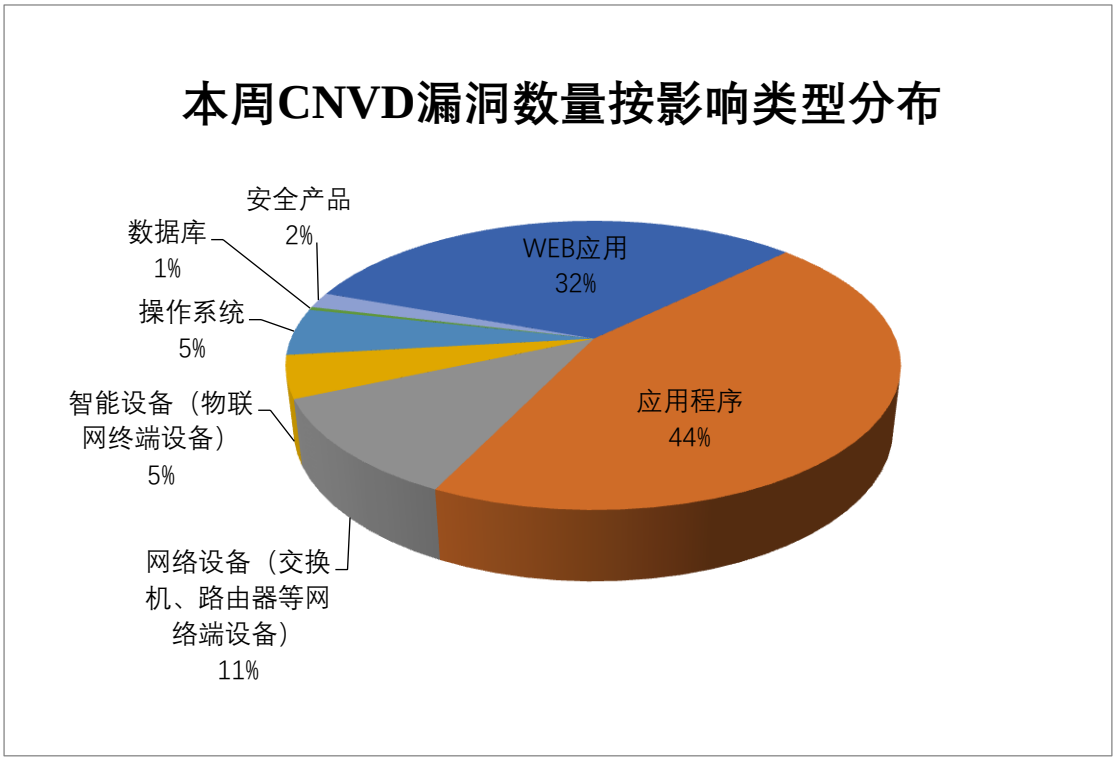

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Bentley Systems、VeryPDF、Jenkins 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	Bentley Systems	48	8%
2	VeryPDF	37	6%
3	Jenkins	33	6%
4	Google	22	4%
5	Adobe	17	3%
6	D-Link	17	3%
7	Oracle	17	3%
8	Tenda	16	3%
9	IBM	12	2%
10	其他	350	62%

本周行业漏洞收录情况

本周，CNVD 收录了 50 个电信行业漏洞，26 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-882 命令注入漏洞、Google Android 权限提升漏洞（CNVD-2022-16342）、TP-Link TL-WR902AC 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/

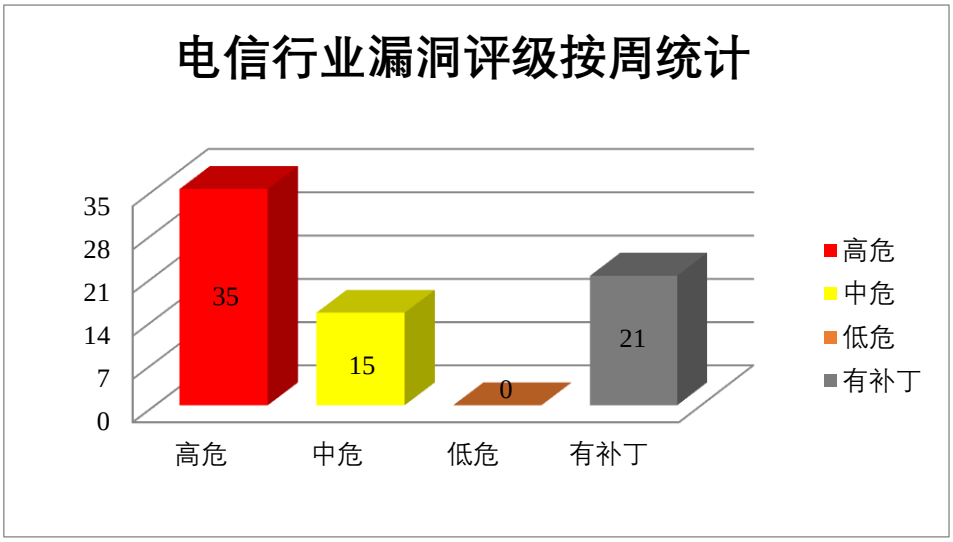

图 3 电信行业漏洞统计

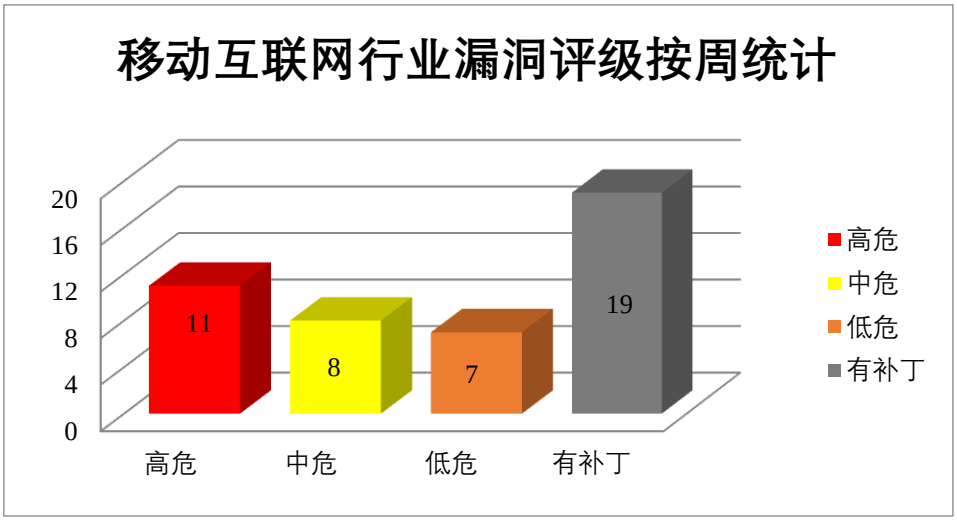

图 4 移动互联网行业漏洞统计

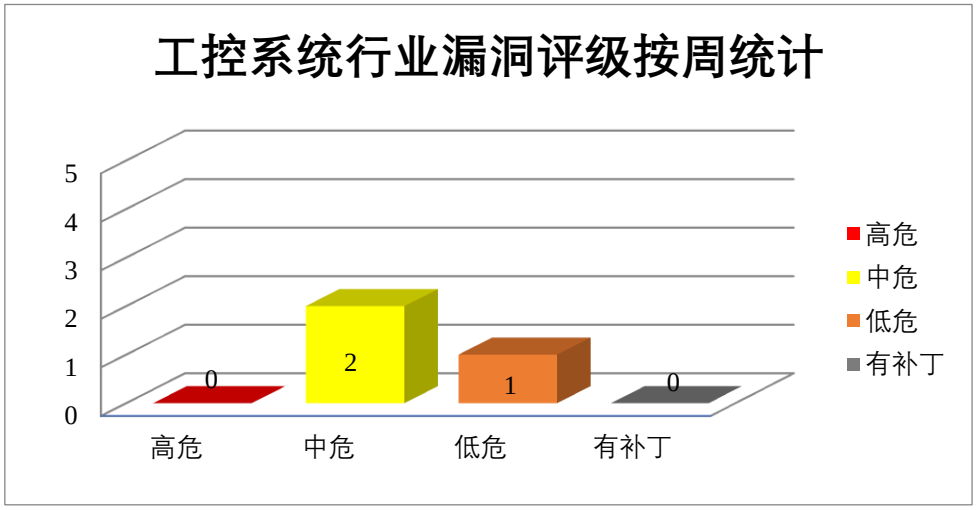

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。本周，上述产品被披露存在越界读取漏洞，攻击者可利用漏洞访问敏感信息。

CNVD 收录的相关漏洞包括：Adobe Illustrator 越界读取漏洞（CNVD-2022-15932、CNVD-2022-15931、CNVD-2022-15934、CNVD-2022-15933、CNVD-2022-15937、CNVD-2022-15936、CNVD-2022-15935、CNVD-2022-15939）。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-2022-15932

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15931

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15934

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15933

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15937

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15936

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15935

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15939

2、 D-Link 产品安全漏洞

D-Link Di-7200G 是中国友讯（D-Link）公司的一款千兆企业级路由器。本周，上述产品被披露存在命令注入漏洞，攻击者可利用漏洞执行任意命令。

CNVD 收录的相关漏洞包括：D-Link DI-7200G 命令注入漏洞（CNVD-2022-15181、

CNVD-2022-15184、CNVD-2022-15183、CNVD-2022-15182、CNVD-2022-15186、CNVD-2022-15185、CNVD-2022-15188、CNVD-2022-15187）。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-2022-15181
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15184
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15183
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15182
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15186
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15185
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15188
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15187

3、Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的的一套以 Linux 为基础的开源操作系统。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多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括 Google Android 竞争条件问题漏洞（CNVD-2022-15197）、Google Android 拒绝服务漏洞（CNVD-2022-15196）、Google Chrome 访问控制错误漏洞（CNVD-2022-16301）、Google Chrome 资源管理错误漏洞（CNVD-2022-16302、CNVD-2022-16304、CNVD-2022-16303）、Google Android 输入验证错误漏洞（CNVD-2022-16337）、Google Android 缓冲区溢出漏洞（CNVD-2022-16338）。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-2022-15197
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15196
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16301
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16302
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16304
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16303
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16337
https://www.cnvd.org.cn/flaw/show/CNVD-2022-16338

4、IBM 产品安全漏洞

IBM Sterling Secure Proxy 是 IBM 公司的一款用于确保组织非保护区（DMZ）中文件安全传输的应用程序代理，通过多因素认证、SSL 会话中断、入站防火墙漏洞修补、协议检查和其他控件来确保可信区域的安全性。IBM i 是美国 IBM 公司的一套运行在 I

BM Power Systems 和 IBM PureSystems 中的操作系统。IBM OPENBMC OP910 是一个 POWER8 和 POWER9 模拟器。IBM Tivoli Key Lifecycle Manager（TKLM）是美国 IBM 公司的一套密钥生命周期管理软件。该软件为存储设备提供密钥存储、密钥维护和密钥生命周期管理等功能。IBM QRadar Network Security 是美国 IBM 公司的一个网络安全管理器。用于提供对网络上的活动和用户的更好的可见性和控制，同时使用深度数据包检查、启发式和基于行为的分析来检测和预防高级威胁。IBM AIX（Advanced Interactive eXecutive）是 IBM 开发的一套 UNIX 操作系统，也可称为 AIX。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，权限提升，导致系统拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Sterling Secure Proxy 缓冲区溢出漏洞、IBM VIOS 输入验证错误漏洞、IBM i 缓冲区溢出漏洞、IBM OPENBMC OP910 信息泄露漏洞、IBM Tivoli Key Lifecycle Manager 信息泄露漏洞（CNVD-2022-15541）、IBM Q Radar Network Security 信息泄露漏洞（CNVD-2022-15539）、IBM AIX 拒绝服务漏洞（CNVD-2022-17018）、IBM AIX 输入验证错误漏洞（CNVD-2022-17017）。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-2022-15533
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15532
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15538
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15536
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15541
https://www.cnvd.org.cn/flaw/show/CNVD-2022-15539
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17018
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17017

5、Tenda G1 and G3 命令注入漏洞（CNVD-2022-16177）

Tenda G1 and G3 是中国腾达（Tenda）公司的一个路由器。本周，Tenda G1 and G3 被披露存在命令注入漏洞。攻击者可利用该漏洞通过 usbOrdinaryUserName 参数执行任意命令。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-2022-16177

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	D-Link Dir-823-Pro 命令注入	高	厂商已发布了漏洞修复程序，请及

-15180	漏洞		时关注更新：https://www.dlink.com/en/security-bulletin
CNVD-2022-15191	Google Android 权限提升漏洞（CNVD-2022-15191）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2022-01-01
CNVD-2022-16300	Airspan Networks Mmp 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cloud.mimosa.co/app/index.html#/updateFirmware/firmwareDownload/MMP
CNVD-2022-15505	Ubiquiti Networks UniFi Protect 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://community.ui.com/releases/Security-Advisory-Bulletin-019-019/90a00abe-d6b6-43c6-92d4-0a0342f1506f
CNVD-2022-16289	Envoy 信任管理问题漏洞（CNVD-2022-16289）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/envoyproxy/envoy/security/advisories/GHSA-837m-wjrv-vm5g
CNVD-2022-16298	Airspan Networks Mmp 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://cloud.mimosa.co/app/index.html#/updateFirmware/firmwareDownload/MMP
CNVD-2022-16402	Spring Cloud Gateway 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：https://spring.io/blog/2022/03/01/spring-cloud-gateway-cve-reports-published
CNVD-2022-17012	Scrapy 信息泄露漏洞（CNVD-2022-17012）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/scrapy/scrapy
CNVD-2022-15189	D-Link DIR-882 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.dlink.com/en/security-bulletin
CNVD-2022-16295	Airspan Networks Mmp 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://cloud.mimosa.co/app/index.html#/updateFirmware/firmwareDownload/MMP

小结：本周，Adobe 产品被披露存在越界读取漏洞，攻击者可利用漏洞访问敏感信息。此外，D-Link、Google、IBM 等多款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，权限提升，执行任意代码，导致拒绝服务等。另外，Tenda G1 and G3 被披露存在命令注入漏洞。攻击者可利用该漏洞通过 usbOrdinaryUserName 参数执行任意命令。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、WordPress 插件 Survey & Poll SQL 注入漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。Survey & Poll 是网站上游客直接反馈的解决方案。

WordPress 插件 Survey & Poll 存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://www.exploit-db.com/exploits/50269

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-16708

信息提供者

深信服科技股份有限公司

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. 近 75%的输液泵受严重漏洞影响

研究人员对来自医院和医疗机构 200000 多个联网输液泵数据进行的分析显示，这些医疗设备中有 75%存在安全漏洞，可能使它们面临潜在的利用风险。

参考链接：https://thehackernews.com/2022/03/report-nearly-75-of-infusion-pumps.html

2. VoIPmonitor 监控软件中发现严重安全漏洞

VoIPmonitor 监控软件中发现了严重的安全漏洞，如果成功利用，可允许未经身份验证的攻击者将权限提升到管理员级别，并执行任意命令。

参考链接：https://thehackernews.com/2022/03/critical-security-bugs-uncovered-in.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