国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 06 月 27 日-2022 年 07 月 03 日 **2022 年第 26 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 439 个，其中高危漏洞 176 个、中危漏洞 211 个、低危漏洞 52 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 322 个（占 73%），其中互联网上出现“Prison Management System SQL 注入漏洞（CNVD-2022-48389）、Sourcecodester Hospital Patient Records Management System SQL 注入漏洞（CNVD-2022-48745）”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 6721 个，与上周（8658 个）环比减少 22%。

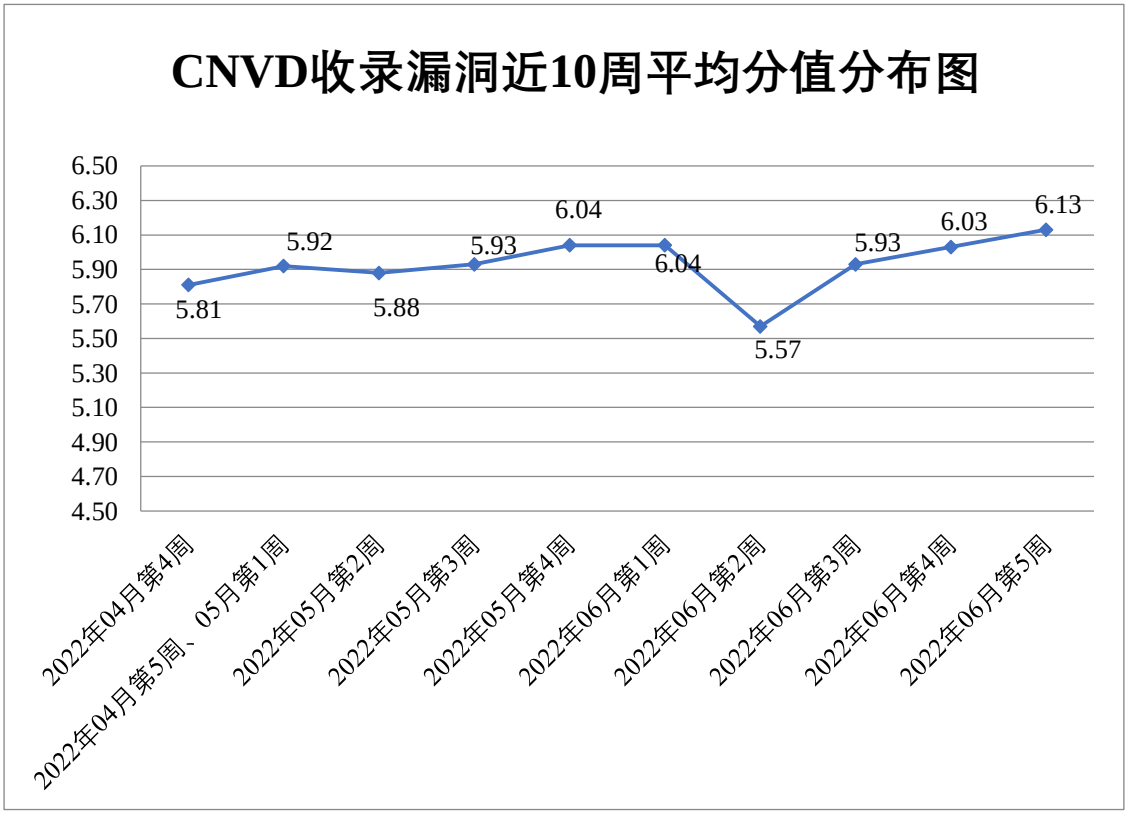

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电信企业通报漏洞事件 24 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 478 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 158 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 95 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：

珠海金山办公软件有限公司、浙江臻善科技股份有限公司、浙江蓝联科技股份有限公司、浙江大华技术股份有限公司、掌如科技服务有限公司、远景能源有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、武汉中地数码科技有限公司、武汉烽火信息集成技术有限公司、微软（中国）有限公司、台达电子企业管理（上海）有限公司、四平市九州易通科技有限公司、思科系统（中国）网络技术有限公司、深圳市异度信息产业有限公司、深圳市唯传科技有限公司、深圳市腾讯计算机系统有限公司、深圳市水务科技有限公司、深圳市水务（集团）有限公司、深圳市科图自动化新技术有限公司、深圳市吉祥腾达科技有限公司、深圳创维数字技术有限公司、深信服科技股份有限公司、上海卓卓网络科技有限公司、上海展盟网络科技有限公司、上海商派网络科技有限公司、上海浪擎信息科技有限公司、上海二三四五移动科技有限公司、山东山大华天软件有限公司、山东金钟科技集团股份有限公司、吉翁电子（深圳）有限公司、湖南翱云网络科技有限公司、恒锋信息科技股份有限公司、合肥图鸭信息科技有限公司、杭州三汇信息工程有限公司、杭州三汇数字信息技术有限公司、桂林崇胜网络科技有限公司、广州中望龙腾软件股份有限公司、广州图创计算机软件开发有限公司、广州酷狗计算机科技有限公司、广州鼎成信息科技有限公司、广联达科技股份有限公司、烽火通信科技股份有限公司、德国倍福自动化有限公司、郸城县新翔软件科技有限公司、畅捷通信息技术股份有限公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京云中融信网络科技有限公司、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、北京数科网维技术有限责任公司、北京瑞星网安技术股份有限公司、北京九思协同软件有限公司、北京国栋科技有限公司、北京辰信领创信息技术有限公司、北京宝兰德软件股份有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、安徽省科大奥锐科技有限公司、中保科技集团、易迅软件工作室、美团安全应急响应中心、万通 CMS、狂雨小说 cms、华夏 ERP、WordPress、WAVLINK、The Apache Software Foundation、Nginx、Linksys、JFinalOA、ImageMagick Studio LLC、Glyph & Cog, LLC、Emerson 和 Adobe。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、杭州安恒信息技术股份有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。上海纽盾科技股份有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州默安科技有限公司、山东新潮信息技术有限公司、河南东方云盾信息技术有限公司、河南信安世纪科技有限公司、江苏省信息安全测评中心、杭州海康威视数字技术股份有限公司、河南灵创电子科技有限公司、北京山石网科信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、重庆都会信息科技、广州安亿信软件科技有限公司、江苏国泰新点软件有限公司、广州百蕴启辰科技有限公司、山石网科通信技术股份有限公司、智网安云（武汉）信息技术有限公司、浙江木链物联网科技有限公司、贵州泰若数字科技有限公司、思而听网络科技有限公司、北京机沃科技有限公司、江苏耘和计算机系统工程有限公司及其他个人白帽子向 CNVD 提交了 6721 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 4900 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）	2309	2309
奇安信网神（补天平台）	2240	2240
深信服科技股份有限公司	441	0
北京神州绿盟科技有限公司	381	0
新华三技术有限公司	371	0
上海交大	351	351
杭州安恒信息技术股份有限公司	295	295
北京数字观星科技有限公司	295	0
安天科技集团股份有限公司	219	0
卫士通信息产业股份有限公司	73	45

恒安嘉新（北京）科技股份公司	60	0
北京启明星辰信息安全技术有限公司	55	0
北京华顺信安科技有限公司	47	0
北京天融信网络安全技术有限公司	41	2
京东科技信息技术有限公司	29	29
中国电信集团系统集成有限责任公司	22	0
西安四叶草信息技术有限公司	14	14
内蒙古云科数据服务股份有限公司	14	14
北京知道创宇信息技术股份有限公司	4	0
上海纽盾科技股份有限公司	17	17
奇安星城网络安全运营服务（长沙）有限公司	15	15
杭州迪普科技股份有限公司	14	0
杭州默安科技有限公司	9	9
山东新潮信息技术有限公司	8	8
河南东方云盾信息技术有限公司	6	6
河南信安世纪科技有限公司	5	5
江苏省信息安全测评中心	4	4

杭州海康威视数字技术股份有限公司	4	4
河南灵创电子科技有限公司	3	3
北京山石网科信息技术有限公司	3	3
北京云科安信科技有限公司（Seraph 安全实验室）	3	3
重庆都会信息科技	2	2
广州安亿信软件科技有限公司	2	2
江苏国泰新点软件有限公司	1	1
广州百蕴启辰科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
智网安云（武汉）信息技术有限公司	1	1
浙江木链物联网科技有限公司	1	1
贵州泰若数字科技有限公司	1	1
思而听网络科技有限公司	1	1
北京机沃科技有限公司	1	1
江苏耘和计算机系统工程有限公司	1	1
亚信科技（成都）有限公司	1	0
CNCERT 宁夏分中心	5	5
CNCERT 浙江分中心	3	3
CNCERT 内蒙古分中	2	2

心		
个人	1322	1322
报送总计	8698	6721

本周漏洞按类型和厂商统计

本周，CNVD 收录了 439 个漏洞。WEB 应用 243 个，应用程序 67 个，网络设备（交换机、路由器等网络端设备）66 个，操作系统 39 个，智能设备（物联网终端设备）17 个，安全产品 5 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
WEB 应用	243
应用程序	67
网络设备（交换机、路由器等网络端设备）	66
操作系统	39
智能设备（物联网终端设备）	17
安全产品	5
数据库	2

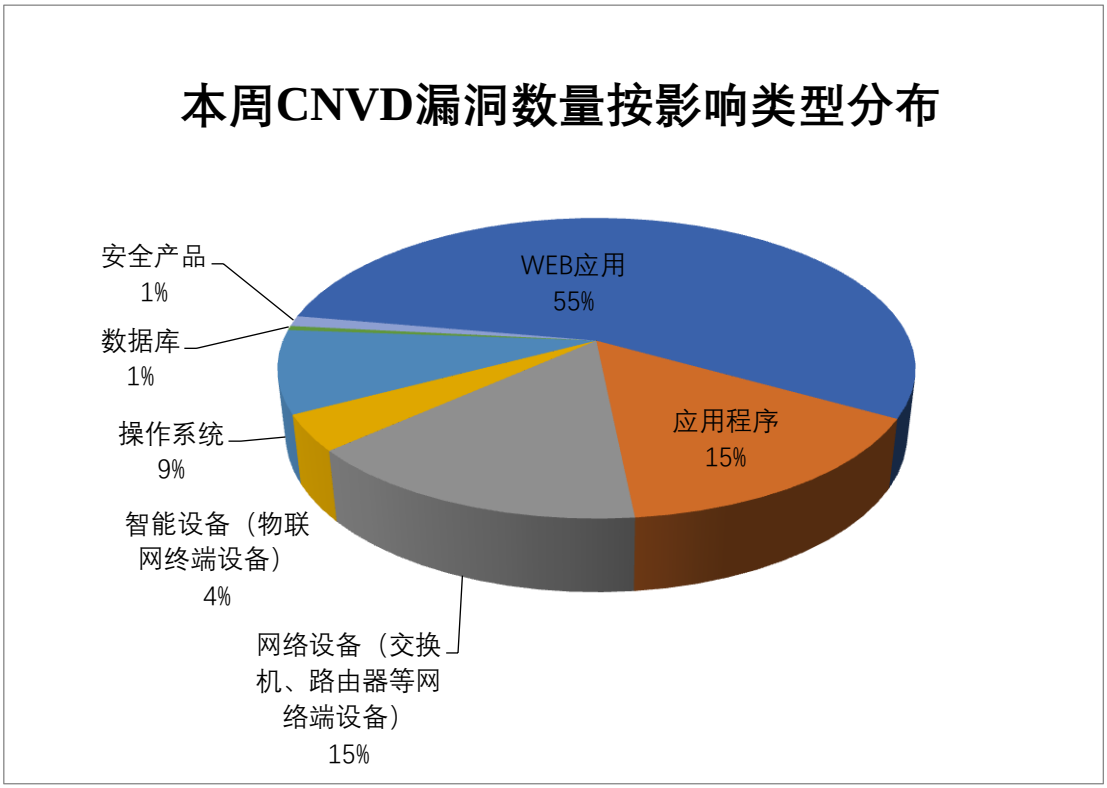

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、SourceCodester、Huawei 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	WordPress	41	9%
2	SourceCodester	22	5%
3	Huawei	21	5%
4	Adobe	20	5%
5	Prison Management System	18	4%
6	Google	16	4%
7	深圳市吉祥腾达科技有限公司	15	3%
8	Complete Online Job Search System	12	3%
9	Fortinet	10	2%
10	其他	264	60%

本周行业漏洞收录情况

本周，CNVD 收录了 48 个电信行业漏洞，32 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，“多款 TotoLink 产品命令注入漏洞（CNVD-2022-47968）、Google Android 资源管理错误漏洞（CNVD-2022-47681）”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/

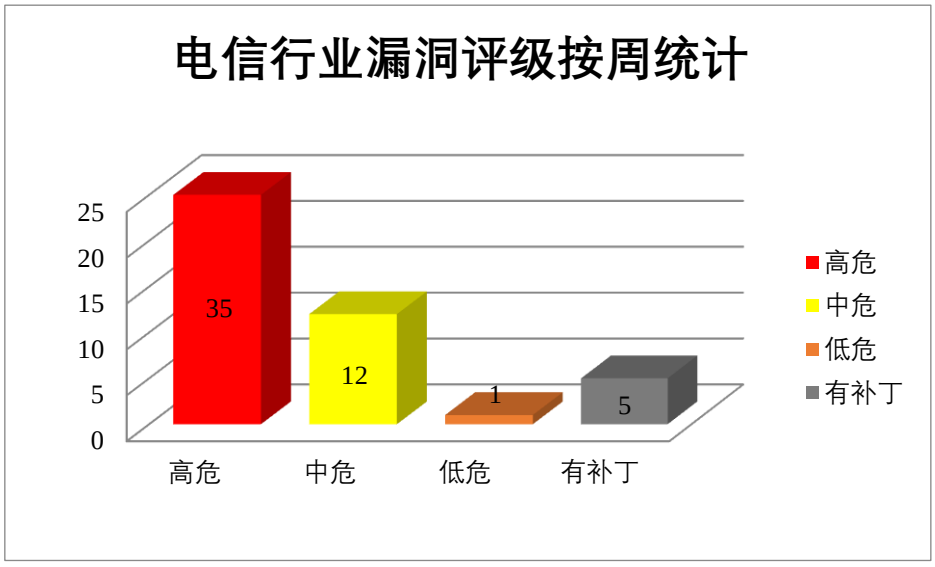

图 3 电信行业漏洞统计

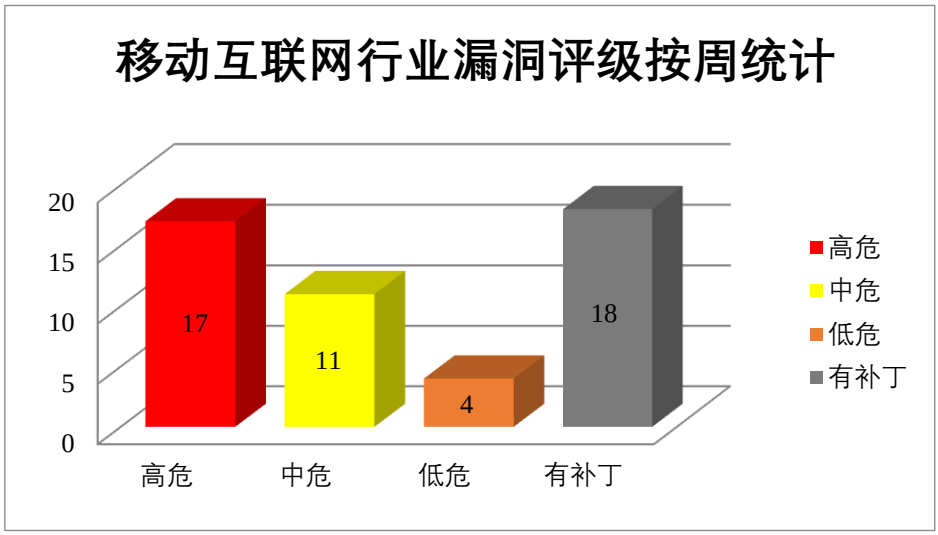

图 4 移动互联网行业漏洞统计

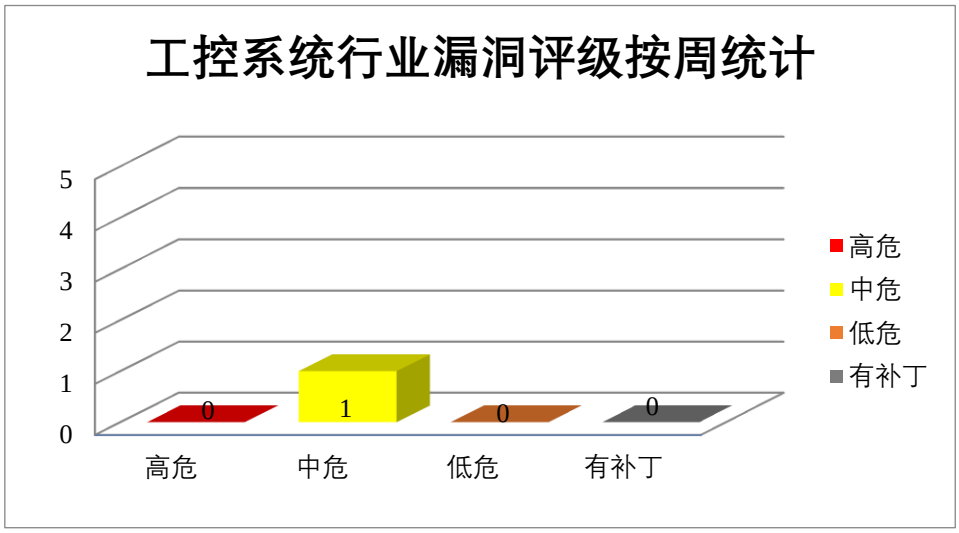

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei CV81-WDM FW 是中国华为（Huawei）公司的一款激光多功能打印机。HUAWEI HarmonyOS 是中国华为（HUAWEI）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。HUAWEI EMUI and Magic UI 是中国华为（HUAWEI）公司的一款基于 Android 开发的移动端操作系统。Huawei FLMG-10 是中国华为（Huawei）公司的一款高端蓝牙遥控音箱。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系统机密，导致拒绝服务，权限提升等。

CNVD 收录的相关漏洞包括：Huawei CV81-WDM FW 拒绝服务漏洞、HUAWEI HarmonyOS 代码问题漏洞（CNVD-2022-47648、CNVD-2022-47651）、HUAWEI EMU

I and Magic UI 信息泄露漏洞、HUAWEI HarmonyOS 资源管理错误漏洞（CNVD-2022-47652）、HUAWEI HarmonyOS 缓冲区溢出漏洞（CNVD-2022-47650）、Huawei FLMG-10 授权问题漏洞、Huawei CV81-WDM FW 缓冲区溢出漏洞。其中，除“HUAWEI HarmonyOS 代码问题漏洞（CNVD-2022-47648、CNVD-2022-47651）、HUAWEI EMUI and Magic UI 信息泄露漏洞”外其余漏洞的综合评级为“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-2022-47649
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47648
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47647
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47652
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47651
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47650
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47655
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47654

2、 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，攻击者可利用漏洞导致本地权限升级。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2022-47668、CNVD-2022-47674、CNVD-2022-47673、CNVD-2022-47675）、Google Android 权限提升漏洞（CNVD-2022-47670、CNVD-2022-47672、CNVD-2022-47680）、Google Android 权限许可和访问控制问题漏洞（CNVD-2022-47677）。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-2022-47668
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47670
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47674
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47673
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47672
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47677
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47675
https://www.cnvd.org.cn/flaw/show/CNVD-2022-47680

3、 Adobe 产品安全漏洞

Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。本周，上述产品被披露存在多个

漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe InDesign 越界写入漏洞（CNVD-2022-48769、CNVD-2022-48767、CNVD-2022-48770、CNVD-2022-48781、CNVD-2022-48780）、Adobe InDesign 堆缓冲区溢出漏洞、Adobe Bridge 越界写入漏洞（CNVD-2022-48774、CNVD-2022-48778）。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-2022-48769

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48768

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48767

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48770

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48774

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48778

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48781

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48780

4、Fortinet 产品安全漏洞

Fortinet FortiEDR 是美国 Fortinet 公司的一个从头开始构建的端点安全解决方案。Fortinet FortiWan 是美国 Fortinet 公司的一个网络设备。用于在不同网络之间执行负载平衡和容错。Fortinet FortiClient 是美国 Fortinet 公司的一种结构代理。用于在单个模块化轻量级客户端中提供保护、合规性和安全访问。Fortinet FortiManager 是一套集中化网络安全管理平台。Fortinet FortiAnalyzer 是一套集中式网络安全报告解决方案。Fortinet FortiPortal 是 FortiGate、FortiWiFi 和 FortiAP 产品线的高级、功能丰富的托管安全分析和管理支持工具，可作为虚拟机供 MSP 使用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪装和伪造来自其他收集器的消息，从同一部署中的端点禁用和卸载收集器，借助特制的 HTTP 请求执行未经授权的代码或命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiEDR 信任管理问题漏洞（CNVD-2022-47976、CNVD-2022-47977）、Fortinet FortiWAN SQL 注入漏洞、Fortinet FortiWAN 加密问题漏洞、Fortinet FortiClient for Linux 信息泄露漏洞、Fortinet 多款产品操作系统命令注入漏洞、Fortinet FortiWAN 操作系统命令注入漏洞、Fortinet FortiWAN 缓冲区溢出漏洞。其中，“Fortinet FortiWAN SQL 注入漏洞、Fortinet 多款产品操作系统命令注入漏洞、Fortinet FortiWAN 操作系统命令注入漏洞、Fortinet FortiWAN 缓冲区溢出漏洞”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-2022-47977

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47976

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47981

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47980

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47979

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47985

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47983

https://www.cnvd.org.cn/flaw/show/CNVD-2022-47982

5、多款 TotoLink 产品命令注入漏洞（CNVD-2022-47973）

Totolink A830R/A3100R/A950RG/A800R/A3000RU/A810R 等产品都是中国 Totolink 公司的路由器。本周，多款 TotoLink 产品被披露存在命令注入漏洞。攻击者可利用该漏洞通过精心制作的请求执行任意命令。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-2022-47973

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-2022-47676	Google Android 权限许可和访问控制问题漏洞（CNVD-2022-47676）	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/2022-03-01
CNVD-2022-47678	Google Android 权限许可和访问控制问题漏洞（CNVD-2022-47678）	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/2022-03-01
CNVD-2022-47682	Google Android 缓冲区溢出漏洞（CNVD-2022-47682）	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/2022-02-01
CNVD-2022-47970	多款 TotoLink 产品命令注入漏洞（CNVD-2022-47970）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/
CNVD-2022-47969	多款 TotoLink 产品命令注入漏洞（CNVD-2022-47969）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/pjqwudi1/my_vuln/blob/main/totolink/vuln_24/24.md
CNVD-2022-47972	多款 TotoLink 产品命令注入漏洞（CNVD-2022-47972）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/pjqwudi1/my_vuln/blob/main/totolink/vuln_28/28.md
CNVD-2022	多款 TotoLink 产品命令注入	高	厂商已发布了漏洞修复程序，请及

-47971	漏洞（CNVD-2022-47971）		时关注更新：https://github.com/pjqwudi1/my_vuln/blob/main/totolink/vuln_27/27.md
CNVD-2022-48171	WordPress Bestbooks plugin SQL 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://wpscan.com/vulnerability/0d208ebc-7805-457b-aa5f-ffd5adb2f3be
CNVD-2022-48381	WordPress Jupiter Theme 和 JupiterX Core Plugin 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://wordpress.org/support/plugin/jupiterx-core/
CNVD-2022-48384	Apache Shiro 身份认证绕过漏洞（CNVD-2022-48384）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/y8260dw8vbm99oq7zv6y3mzn5ovk90xh

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用漏洞获取系统机密，导致拒绝服务，权限提升等。此外，Google、Adobe、Fortinet 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升级，伪装和伪造来自其他收集器的消息，从同一部署中的端点禁用和卸载收集器，借助特制的 HTTP 请求执行未经授权的代码或命令等。另外，多款 TotoLink 产品被披露存在命令注入漏洞。攻击者可利用漏洞通过精心制作的请求执行任意命令。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、Prison Management System SQL 注入漏洞（CNVD-2022-48389）

验证描述

Prison Management System 是 Carlo Montero 个人开发者的一个监狱管理系统。

Prison Management System v1.0 版本存在 SQL 注入漏洞，该漏洞源于应用中/pms/admin/actions/manage_action.php 中的 id 参数缺少 SQL 数据的过滤转义，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/Dyrandy/BugBounty/blob/main/pms/cve-2022-32392.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-48389

信息提供者

新华三技术有限公司

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. 谷歌分析 2022 在野 0day 利用情况：一半以上为修复不完全导致

6 月，谷歌零日项目团队 (Project Zero) 研究员 Maddle Stone 在近期举办的 FIRST 会议上发表了报告《目前为止的 2022 年在野 0day 利用》分享了该团队的对 2022 年上半年 0day 利用情况的研究成果。在 2022 年上半年已遭利用的 0day 中，至少有一半本可通过更全面的打补丁和回归测试得以阻止。

参考链接：https://www.secrss.com/articles/44245

2. 微软在数百个 Windows 网络中发现了蠕虫病毒

微软表示，最近在数百个不同行业组织的网络中发现了 Windows 蠕虫病毒。这种恶意软件被称为“树莓罗宾”(Raspberry Robin)，通过受感染的 USB 设备传播。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-finds-raspberry-robin-worm-in-hundreds-of-windows-networks/

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