国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 09 月 19 日-2022 年 09 月 25 日 **2022 年第 38 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 600 个，其中高危漏洞 191 个、中危漏洞 340 个、低危漏洞 69 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 345 个（占 58%），其中互联网上出现“Delta Electronics DIAEnergie 跨站脚本漏洞、WordPress Advanced Uploader plugin 任意文件上传漏洞”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漏洞总数 27685 个，与上周（12967 个）环比增加 114%。

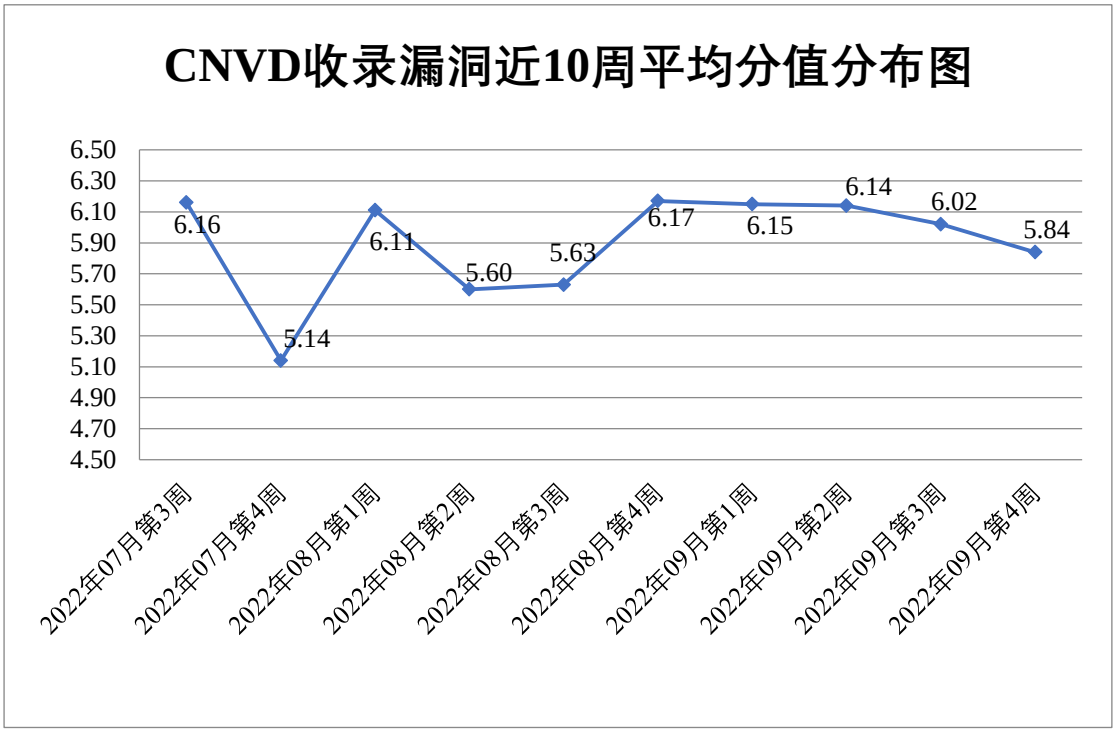

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 35 起，向基础电信企业通报漏洞事件 53 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 825 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 258 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 90 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：

重庆中联信息产业有限责任公司、中青网新媒体科技（北京）有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、云蚁智联（上海）信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、元伸科技（股）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、新天科技股份有限公司、西安丝路智慧科技有限公司、西安旌旗电子股份有限公司、武汉达梦数据库有限公司、潍坊点睛网络科技有限公司、铁岭旭日农业技术开发有限公司、天维尔信息科技股份有限公司、苏州国网电子科技有限公司、四平市九州易通科技有限公司、神州数码控股有限公司、深圳市思迅软件股份有限公司、深圳市普顺达科技有限公司、深圳市捷易科技有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市河湾科技有限公司、深圳市必联电子有限公司、深圳齐心好视通云计算有限公司、深圳昆仑通态科技有限责任公司、深圳华视美达信息技术有限公司、尚思卓越（北京）科技有限公司、上海卓卓网络科技有限公司、上海迅时通信设备有限公司、上海申石软件有限公司、上海快快查信息科技有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海贝锐信息科技股份有限公司、熵基科技股份有限公司、山西复盛公健康药业有限公司、山石网科通信技术（北京）有限公司、山东欧倍尔软件科技有限责任公司、山东卡尔电气股份有限公司、厦门泰博科技有限公司、厦门乐域网络科技有限公司、厦门快普信息技术有限公司、厦门科汛软件有限公司、厦门科拓通讯技术股份有限公司、全讯汇聚网络科技（北京）有限公司、普联技术有限公司、宁夏智林智能科技有限公司、南宁迈世信息技术有限公司、联奕科技股份有限公司、联想（北京）有限公司、乐星电气（无锡）有限公司、浪潮通用软件有限公司、浪潮电子信息产业股份有限公司、朗坤智慧科技股份有限公司、京信网络系统股份有限公司、金蝶天燕云计算股份有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、吉翁电子（深圳）有限公司、华硕电脑（上海）有限公司、湖南建研信息技术股份有限公司、湖南翱云网络科技有限公司、恒锋信息科技股份有限公司、杭州易锐普软件科技有限公司、杭州雄伟科技开发股份有限公司、杭州吉拉科技有限公司、汉王科技股份有限公司、海南有趣科技有限公司、海纳医信（北京）软件科技有限责任公司、桂林崇胜网络科技有限公司、贵阳思普信息技术有限公司、广州小橘灯信息科技有限公司、广州网视通信息科技有限公司、广州鼎甲计算机科技有限公司、广东飞企互联科技股份有限公司、福州目雪科技有限公司、福州金网际软件开

发有限公司、佛山市顺德区出格软件设计有限公司、帝国软件、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、成都任我行软件股份有限公司、畅捷通信息技术股份有限公司、北京中新天达科技有限公司、北京中广上洋科技股份有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京伟联科技有限公司、北京网御星云信息技术有限公司、北京万维盈创科技发展有限公司、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京数科网维技术有限责任公司、北京神州视翰科技有限公司、北京启明星辰信息安全技术有限公司、北京梦见星科技有限公司、北京联达动力信息科技股份有限公司、北京立达悦胜科技有限公司、北京快手科技有限公司、北京久幺幺科技有限公司、北京宏景世纪软件股份有限公司、北京和欣运达科技有限公司、北京点聚信息技术有限公司、北京弹幕网络科技有限公司、北京辰信领创信息技术有限公司、北京缤纷竹林科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司和安美世纪（北京）科技有限公司。

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、新华三技术有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、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、江苏保旺达软件技术有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、北京山石网科信息技术有限公司、江西和尔惠信息技术有限公司、山石网科通信技术股份有限公司、长春嘉诚信息技术股份有限公司、重庆都会信息科技、浙江木链物联网科技有限公司、中能融合智慧科技有限公司、上海纽盾科技股份有限公司、北京君云天下科技有限公司、苏州棱镜七彩信息科技有限公司、广州安亿信软件科技有限公司、湖北珞格科技发展有限公司、西藏熙安信息技术有限责任公司、金蝶软件（中国）有限公司、北京快手科技有限公司、北京升鑫网络科技有限公司、杭州美创科技有限公司、成方金融科技有限公司上海分公司、中国电信股份有限公司上海研究院、河南灵创电子科技有限公司、中国电信股份有限公司网络安全产品运营中心及其他个人白帽子向 CNVD 提交了 27685 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）、三六零数字安全科技集团有限公司、奇安信网神（补天平台）和上海交大向 CNVD 共享的白帽子报送的 25757 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
奇安信网神（补天平	17907	17907

台）		
斗象科技（漏洞盒子）	5199	5199
三六零数字安全科技集团有限公司	2014	2014
上海交大	637	637
深信服科技股份有限公司	557	0
新华三技术有限公司	425	0
安天科技集团股份有限公司	236	0
北京神州绿盟科技有限公司	219	4
北京数字观星科技有限公司	201	0
阿里云计算有限公司	201	0
南京众智维信息科技有限公司	189	189
杭州安恒信息技术股份有限公司	160	108
恒安嘉新（北京）科技股份公司	102	0
西安四叶草信息技术有限公司	101	101
北京天融信网络安全技术有限公司	100	0
卫士通信息产业股份有限公司	77	77
北京启明星辰信息安全技术有限公司	65	9
天津市国瑞数码安全系统股份有限公司	59	0
远江盛邦（北京）网络安全科技股份有限公司	43	43
中国电信集团系统集	34	4

成有限责任公司		
北京知道创宇信息技术有限公司	15	1
京东科技信息技术有限公司	13	0
浙江大华技术股份有限公司	3	3
北京智游网安科技有限公司	3	3
北京长亭科技有限公司	3	3
北京知道创宇信息技术股份有限公司	3	0
沈阳东软系统集成工程有限公司	2	2
北京华顺信安信息技术有限公司	216	5
杭州迪普科技股份有限公司	41	0
奇安星城网络安全运营服务（长沙）有限公司	33	33
杭州默安科技有限公司	20	20
江苏保旺达软件技术有限公司	17	17
山东云天安全技术有限公司	15	15
河南信安世纪科技有限公司	15	15
快页信息技术有限公司	10	10
河南东方云盾信息技术有限公司	10	10
北京山石网科信息技	10	10

术有限公司		
江西和尔惠信息技术有限公司	6	6
山石网科通信技术股份有限公司	5	5
长春嘉诚信息技术股份有限公司	5	5
重庆都会信息科技	4	4
浙江木链物联网科技有限公司	3	3
中能融合智慧科技有限公司	3	3
上海纽盾科技股份有限公司	3	3
北京君云天下科技有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
湖北珞格科技发展有限公司	2	2
西藏熙安信息技术有限责任公司	1	1
金蝶软件（中国）有限公司	1	1
北京快手科技有限公司	1	1
北京升鑫网络科技有限公司	1	1
杭州美创科技有限公司	1	1
成方金融科技有限公司上海分公司	1	1
中国电信股份有限公	1	1

司上海研究院		
河南灵创电子科技有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	1	1
亚信科技（成都）有限公司	1	0
CNCERT 宁夏分中心	5	5
CNCERT 贵州分中心	3	3
个人	1192	1192
报送总计	30202	27685

本周漏洞按类型和厂商统计

本周，CNVD 收录了 600 个漏洞。WEB 应用 280 个，应用程序 183 个，网络设备（交换机、路由器等网络端设备）76 个，数据库 18 个，操作系统 17 个，智能设备（物联网终端设备）16 个，安全产品 10 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	280
应用程序	183
网络设备（交换机、路由器等网络端设备）	76
数据库	18
操作系统	17
智能设备（物联网终端设备）	16
安全产品	10

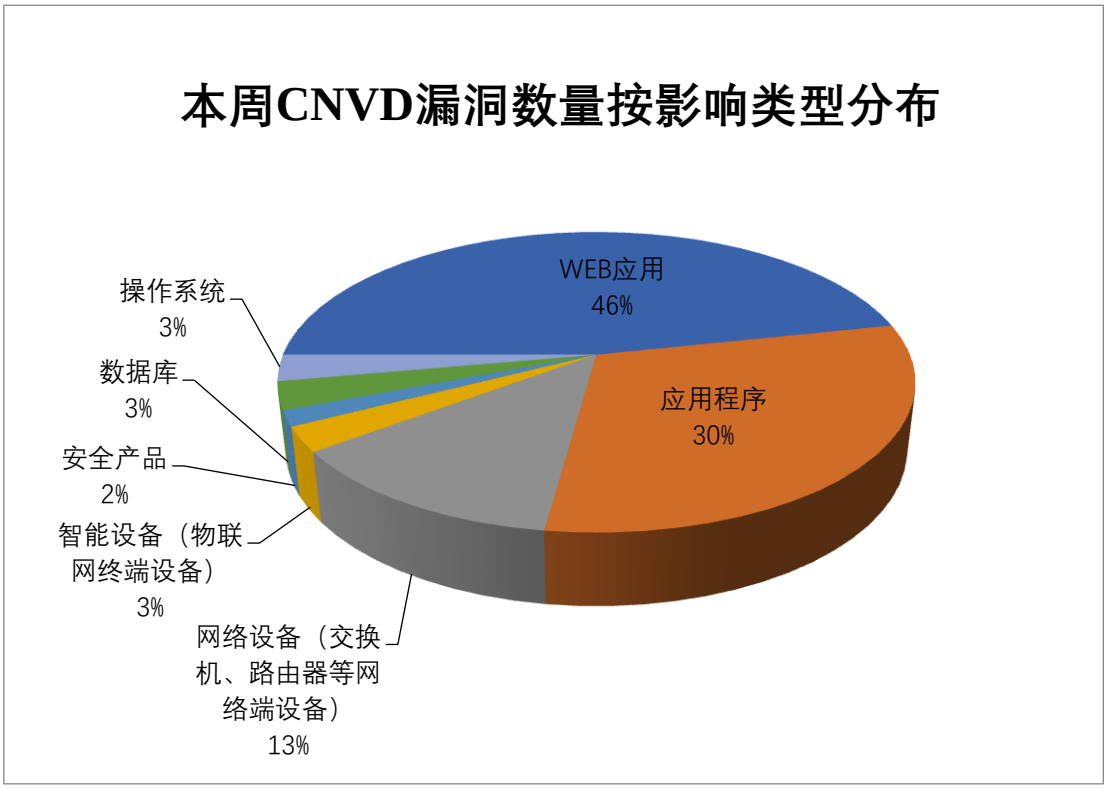

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Google、D-Link 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	7%
2	Google	36	6%
3	D-Link	31	5%
4	MariaDB	18	3%
5	Samsung	16	3%
6	Huawei	14	2%
7	Mattermost	13	2%
8	TOTOLINK	13	2%
9	Adobe	10	2%
10	其他	408	68%

本周行业漏洞收录情况

本周，CNVD 收录了 62 个电信行业漏洞，36 个移动互联网行业漏洞，22 个工控行业漏洞（如下图所示）。其中，“TOTOLINK A7100RU 命令注入漏洞、Secheron SEP COS Control and Protection Relay 权限提升漏洞”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/

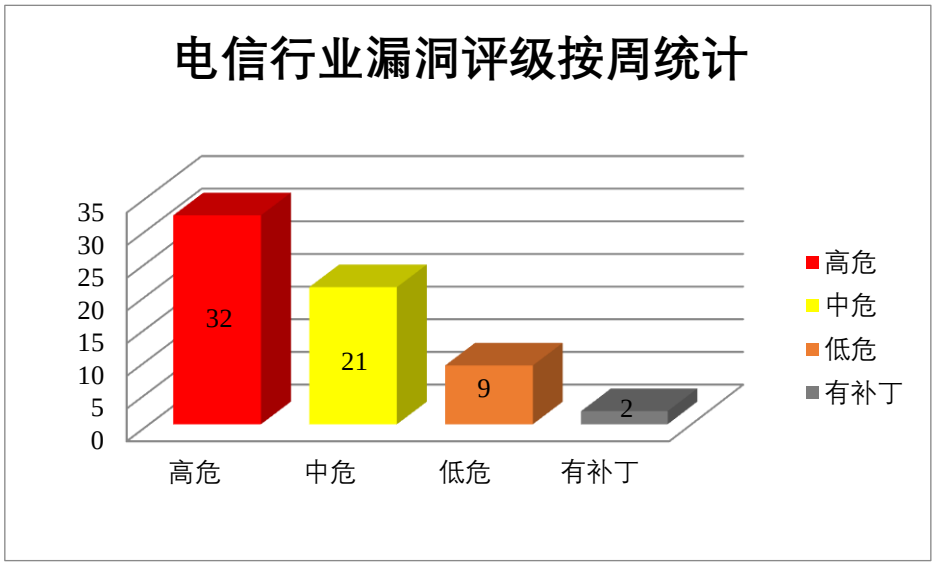

图 3 电信行业漏洞统计

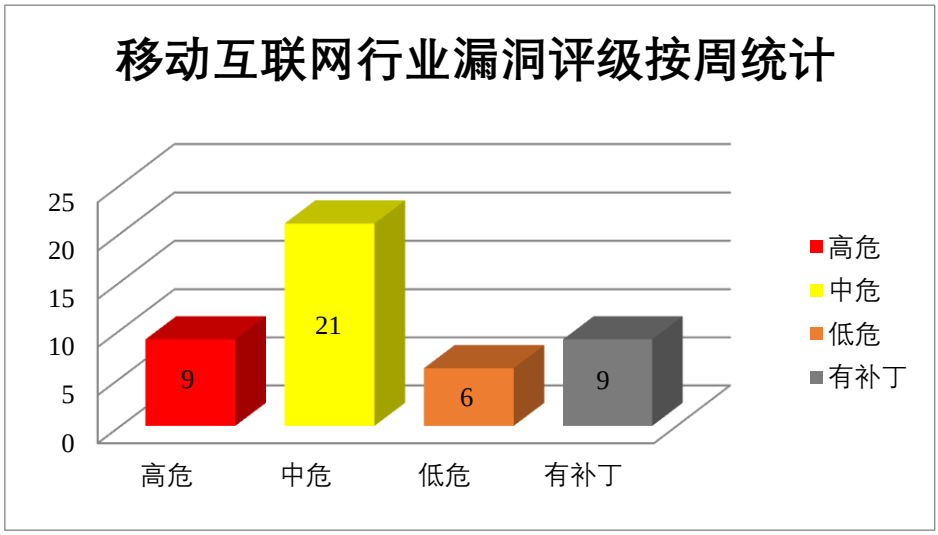

图 4 移动互联网行业漏洞统计

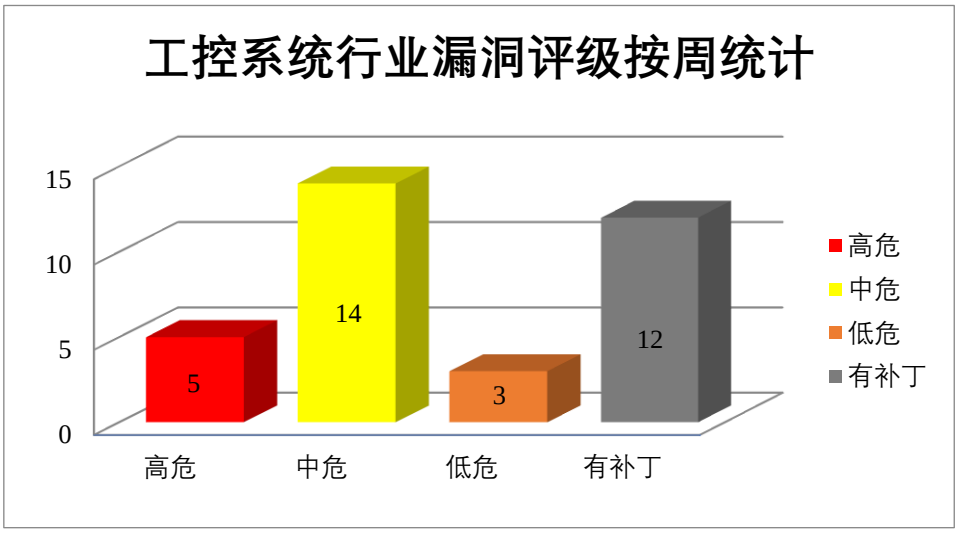

图 5 工控系统行业漏洞统计

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 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，攻击者可利用漏洞在系统上执行任意代码或造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Google Chrome WebShare 内存错误引用漏洞、Google Chrome Mojo 代码执行漏洞（CNVD-2022-63925）、Google Chrome Omnibox 代码执行漏洞、Google Chrome OS Shell 内存错误引用漏洞、Google Chrome Views 代码执行漏洞、Google Chrome Cast UI 内存错误引用漏洞、Google Chrome MediaStream 内存错误引用漏洞、Google Chrome Media 内存错误引用漏洞（CNVD-2022-63926）。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-2022-63921

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63925

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63924

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63923

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63922

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63928

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63927

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63926

2、 Samsung 产品安全漏洞

Samsung SMR 是韩国三星（Samsung）公司的一个系统补丁包。提供了三星手机应

用的补丁程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞启动某些活动，导致越界写入。

CNVD 收录的相关漏洞包括：Samsung SMR 代码问题漏洞（CNVD-2022-64247、CNVD-2022-64248、CNVD-2022-64250、CNVD-2022-64249）、Samsung SMR 输入验证错误漏洞（CNVD-2022-64252、CNVD-2022-64251、CNVD-2022-64254、CNVD-2022-64253）。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-2022-64247
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64248
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64250
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64249
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64252
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64251
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64254
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64253

3、 Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe InCopy 是 Adobe 公司出品的一个应用程序，用于专业的文字处理。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进程的上下文中执行代码，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：Adobe Bridge 缓冲区溢出漏洞（CNVD-2022-64963、CNVD-2022-64966、CNVD-2022-64965、CNVD-2022-64964、CNVD-2022-64968、CNVD-2022-64967）、Adobe InCopy 缓冲区溢出漏洞（CNVD-2022-64971、CNVD-2022-64970）。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-2022-64963
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64966
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64965
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64964
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64968
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64967
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64971
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64970

4、 Huawei 产品安全漏洞

Huawei EMUI 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 EMUI/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 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。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越界访问，在系统上执行任意代码，导致权限提升等。

CNVD 收录的相关漏洞包括：Huawei EMUI 代码执行漏洞（CNVD-2022-64481）、Huawei EMUI and Magic UI 缓冲区溢出漏洞、Huawei HarmonyOS 缓冲区溢出漏洞（CNVD-2022-64981）、Huawei HarmonyOS 反序列化漏洞、Huawei HarmonyOS WLAN 模块信息泄露漏洞、Huawei HarmonyOS WLAN 模块授权问题漏洞、Huawei HarmonyOS 权限提升漏洞（CNVD-2022-64985）、Huawei HarmonyOS 配置错误漏洞。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-2022-64481
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64977
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64981
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64980
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64979
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64978
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64985
https://www.cnvd.org.cn/flaw/show/CNVD-2022-64984

5、D-Link DIR-816 缓冲区溢出漏洞（CNVD-2022-64487）

D-Link DIR-816 是中国台湾友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-816 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致系统崩溃。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-2022-64487

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：https://www.cnvd.org.cn/flaw/list

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-2022-64083	Samsung Galaxy Store 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=07
CNVD-2022-64102	Joomla! SQL 注入漏洞（CNVD-2022-64102）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://developer.joomla.org/security-c

			entre/874-20220305-core-inadequate-filtering-on-the-selected-ids.html
CNVD-2022-64108	ASG technologies ASG-Zena Cross Platform Server Enterprise Edition XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.rocketsoftware.com/bundle/ven1649700711249/page/ayk1652945111726.html
CNVD-2022-64111	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar 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://github.com/creativesaiful/Ecommerce-project-with-php-and-mysqli-Fruits-Bazar-
CNVD-2022-64232	Aruba ClearPass Policy Manager 身份验证绕过漏洞（CNVD-2022-64232）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-007.txt
CNVD-2022-64234	Aruba ClearPass Policy Manager 远程身份验证绕过漏洞（CNVD-2022-64234）	高	厂商已发布了漏洞修复程序，请及时关注更新 https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-007.txt
CNVD-2022-64235	Cambium Networks cnMaestro 操作系统命令注入漏洞（CNVD-2022-64235）	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.cambiumnetworks.com/
CNVD-2022-64238	Cambium Networks cnMaestro 操作系统命令注入漏洞（CNVD-2022-64238）	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.cambiumnetworks.com/
CNVD-2022-64237	Cambium Networks cnMaestro 操作系统命令注入漏洞（CNVD-2022-64237）	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.cambiumnetworks.com/
CNVD-2022-64241	Cambium Networks cnMaestro 操作系统命令注入漏洞	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://www.cambiumnetworks.com/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码或造成拒绝服务情况等。此外，Samsung、Adobe、Huawei 等多款产品被披露存在多个漏洞，攻击者可利用漏洞启动某些活动，导致越界写入，当前进程的上下文中执行代码，导致缓冲区溢出等。另外，D-Link DIR-816 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致系统崩溃。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、Delta Electronics DIAEnergie 跨站脚本漏洞

验证描述

Delta Electronics DIAEnergie 是一个工业能源管理系统，用于实时监控和分析能源消耗、计算能源消耗和负载特性、优化设备性能、改进生产流程并最大限度地提高能源效率。

Delta Electronics DIAEnergie v1.08.00 版本存在跨站脚本漏洞，该漏洞源于 System Settings/IOT Settings 模块存在跨站脚本漏洞。攻击者可利用漏洞将特制数据包注入 Name 文本域，执行任意 web 脚本。

验证信息

POC 链接：https://github.com/ZhuoNiBa/Delta-DIAEnergie-XSS

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-65312

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. 澳大利亚 Optus 遭受网络攻击，多达 900 万用户受影响

Optus 透露，它受到了一次网络攻击，导致当前和以前客户的信息被非法获取，包括姓名、出生日期、机密身份证件和电子邮箱地址。

参考链接：https://www.cnbeta.com/articles/tech/1319717.htm

2. 微软 SQL 服务器在 TargetCompany 勒索软件攻击中遭到黑客攻击

安全研究人员警告说，易受攻击的 Microsoft SQL 服务器正成为 FARGO 勒索软件新一轮攻击的目标。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-in-targetcompany-ransomware-attacks/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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