国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 07 月 25 日-2022 年 07 月 31 日 **2022 年第 30 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 622 个，其中高危漏洞 181 个、中危漏洞 243 个、低危漏洞 198 个。漏洞平均分值为 5.14。本周收录的漏洞中，涉及 0day 漏洞 470 个（占 76%），其中互联网上出现“Rescue Dispatch Management System SQL 注入漏洞（CNVD-2022-53913）、TOTOLINK EX1200T 命令注入漏洞”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 7660 个，与上周（10876 个）环比减少 30%。

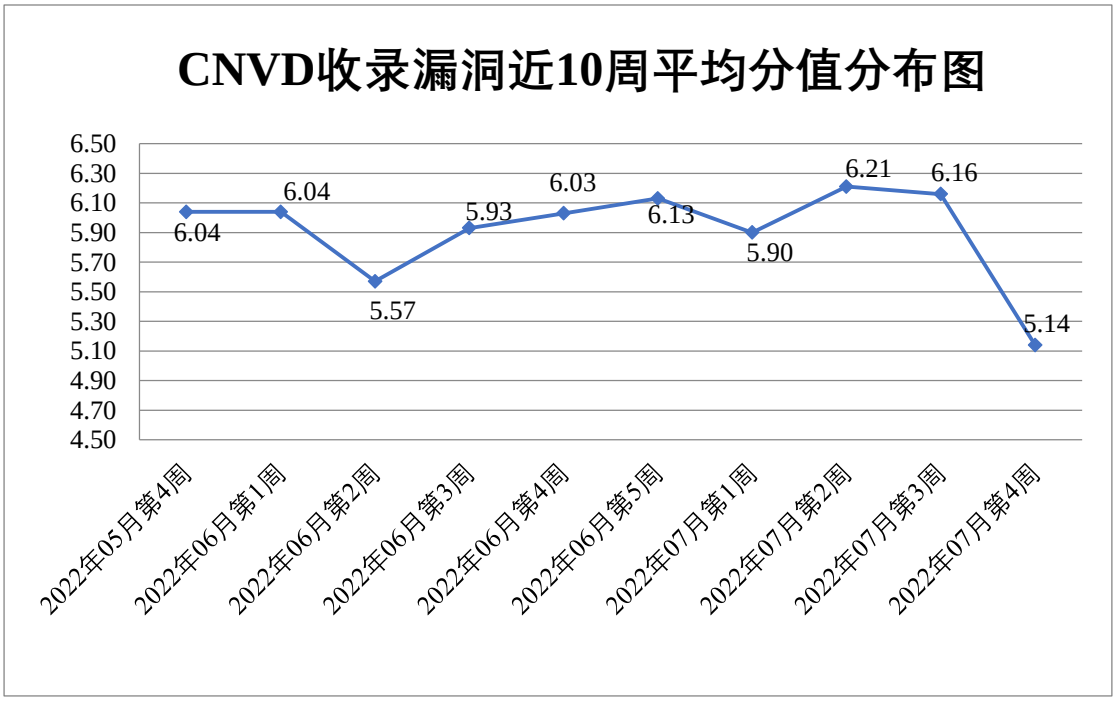

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电

信企业通报漏洞事件 8 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 311 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 70 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 50 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：

珠海高凌信息科技有限公司、重庆远秋科技股份有限公司、重庆米未科技有限公司、中兴通讯股份有限公司、中通客车股份有限公司、中联重科股份有限公司、中科宇图科技股份有限公司、智点汇融科技发展（北京）有限公司、浙江大华技术股份有限公司、长沙市同迅计算机科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、银川方达电子系统工程有限公司、徐州海派科技有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、维沃移动通信有限公司、宿州市涛盛网络科技有限公司、宿迁鑫潮信息技术有限公司、苏州科达科技股份有限公司、苏州汉明科技有限公司、石家庄博士德软件科技开发有限公司、神州数码集团股份有限公司、深圳微羽智能科技有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市昂捷信息技术股份有限公司、上海卓卓网络科技有限公司、上海上业信息科技股份有限公司、上海商汤智能科技有限公司、上海茸易科技有限公司、山西供销农芯乐电子商务有限公司、三未信安科技股份有限公司、任子行网络技术股份有限公司、普联技术有限公司、南京小巨人信息技术有限公司、南京安元科技有限公司、美国谷歌（Google）公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、弘扬软件股份有限公司、恒盛致远（北京）金融信息服务有限公司、河南云拓智能科技有限公司、杭州叙简科技股份有限公司、杭州新视窗信息技术有限公司、杭州海康威视数字技术股份有限公司、海纳医信（北京）软件科技有限责任公司、哈尔滨伟成科技有限公司、国电联合动力技术有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广州红帆科技有限公司、广东轩辕网络科技股份有限公司、东北中油石化有限公司、成都云祺科技有限公司、郴州帝云网络科技有限公司、北京紫荆视通科技有限公司、北京云帆互联科技有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京世纪超星信息技术发展有限责任公司、北京神州绿盟科技有限公司、北京巧巧时代网络科技有限公司、北京派网软件有限公司、北京九思协同软件有限公司、北京捷思锐科技股份有限公司、北京火星高科数字科技有限公司、北京华耀科技有限公司、北京海腾时代科技有限公司、北京富邦融信国际贸易有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、帝国软件、Zebra Technologies、XpdfReader、TRENDnet、The Apache Software Foundation、Python Software Foundation、Nginx、Catfish CMS 和 Axis Communications AB。

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、深信服科技股份有限公司、北京启明星辰信息安全技术有限公司、安天科技集团股份有限公司、恒安嘉新（北京）科技股份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、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、山石网科通信技术股份有限公司、河南信安世纪科技有限公司、河南灵创电子科技有限公司、北京冠程科技有限公司、西安交大捷普网络科技有限公司、苏州棱镜七彩信息科技有限公司、北京安帝科技有限公司、重庆都会信息科技有限公司、长春嘉诚信息技术股份有限公司、广州易东信息安全技术有限公司、中国烟草总公司湖北省公司、湖北珞格科技发展有限公司、任子行网络技术股份有限公司、北京安盟信息技术股份有限公司、贵州泰若数字科技有限公司、广州安亿信软件科技有限公司、墨菲未来科技（北京）有限公司、北京山石网科信息技术有限公司、博智安全科技股份有限公司、南瑞集团公司（国网电力科学研究院）、江苏国泰新点软件有限公司、北京赛博网安科技有限责任公司、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、中国银行及其他个人白帽子向 CNVD 提交了 7660 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 6091 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（补天平台）	2746	2746
斗象科技（漏洞盒子）	2152	2152
三六零数字安全科技集团有限公司	947	947
新华三技术有限公司	328	0
深信服科技股份有限公司	256	1
上海交大	246	246
北京启明星辰信息安全技术有限公司	231	183
安天科技集团股份有限公司	207	0
恒安嘉新（北京）科技股份公司	121	0

北京天融信网络安全技术有限公司	100	1
中国电信集团系统集成有限责任公司	30	0
杭州安恒信息技术股份有限公司	27	27
南京众智维信息科技有限公司	24	24
北京知道创宇信息技术有限公司	17	0
内蒙古奥创科技有限公司	6	6
北京神州绿盟科技有限公司	5	5
西安四叶草信息技术有限公司	2	2
北京华顺信安科技有限公司	213	9
杭州默安科技有限公司	180	180
山东新潮信息技术有限公司	61	61
河南东方云盾信息技术有限公司	34	34
山石网科通信技术股份有限公司	25	25
河南信安世纪科技有限公司	17	17
河南灵创电子科技有限公司	10	10
杭州迪普科技股份有限公司	9	0
北京冠程科技有限公司	7	7
西安交大捷普网络科	5	5

技有限公司		
苏州棱镜七彩信息科技有限公司	5	5
北京安帝科技有限公司	5	5
重庆都会信息科技有限公司	4	4
长春嘉诚信息技术股份有限公司	4	4
广州易东信息安全技术有限公司	4	4
中国烟草总公司湖北省公司	3	3
湖北珞格科技发展有限公司	3	3
任子行网络技术股份有限公司	2	2
北京安盟信息技术股份有限公司	2	2
贵州泰若数字科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
墨菲未来科技（北京）有限公司	1	1
北京山石网科信息技术有限公司	1	1
博智安全科技股份有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
江苏国泰新点软件有限公司	1	1
北京赛博网安科技有限责任公司	1	1

上海纽盾科技股份有限公司	1	1
奇安星城网络安全运营服务（长沙）有限公司	1	1
中国银行	1	1
CNCERT 贵州分中心	5	5
CNCERT 内蒙古分中心	4	4
个人	918	918
报送总计	8978	7660

本周漏洞按类型和厂商统计

本周，CNVD 收录了 622 个漏洞。应用程序 234 个，WEB 应用 230 个，网络设备（交换机、路由器等网络端设备）86 个，操作系统 49 个，数据库 14 个，安全产品 5 个，智能设备（物联网终端设备）4 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	234
WEB 应用	230
网络设备（交换机、路由器等网络端设备）	86
操作系统	49
数据库	14
安全产品	5
智能设备（物联网终端设备）	4

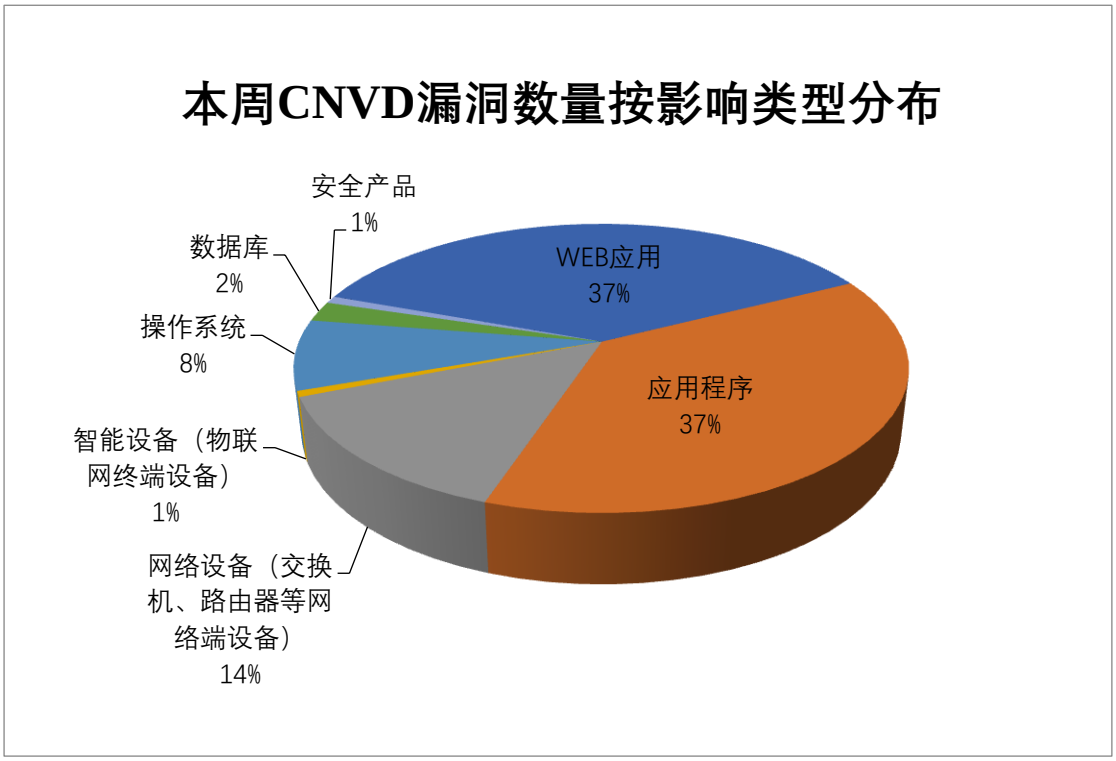

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Carlo Montero、Google、TOTOLINK 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	Carlo Montero	28	5%
2	Google	27	4%
3	TOTOLINK	24	4%
4	WordPress	23	4%
5	Jenkins	20	3%
6	John Paul Lim Gabule	20	3%
7	麒麟软件有限公司	14	2%
8	Cybozu	14	2%
9	Oracle	10	2%
10	其他	442	71%

本周行业漏洞收录情况

本周，CNVD 收录了 63 个电信行业漏洞，55 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，“Google Android 缓冲区溢出漏洞（CNVD-2022-53367）、TOTOLINK N600R 命令注入漏洞（CNVD-2022-53559）”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/

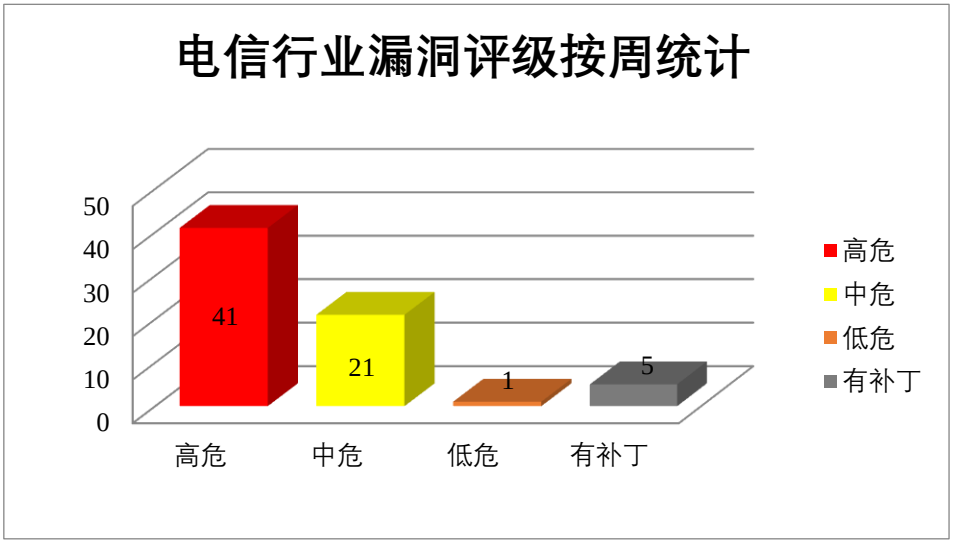

图 3 电信行业漏洞统计

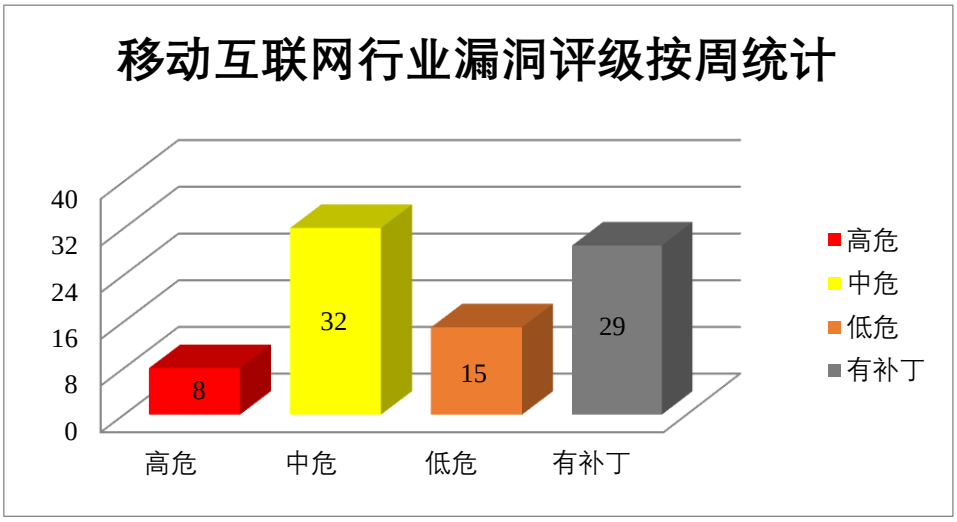

图 4 移动互联网行业漏洞统计

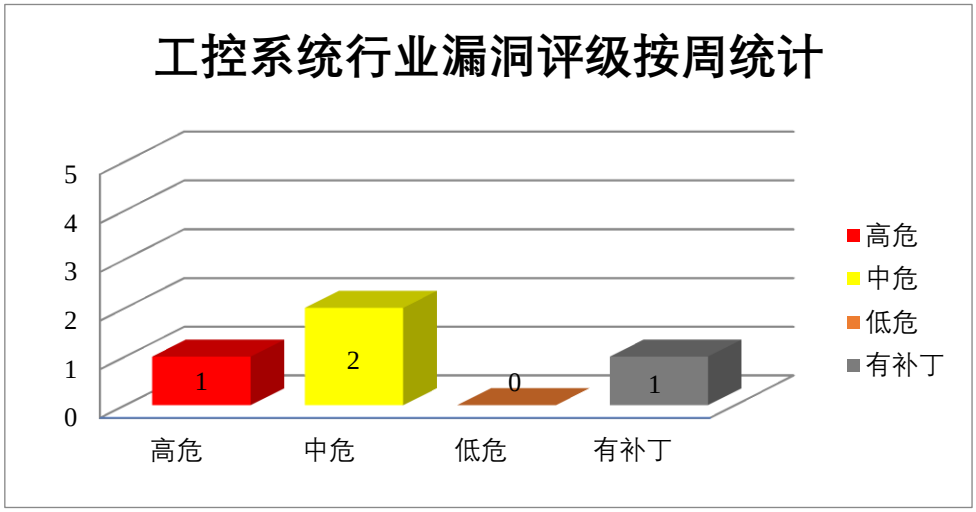

图 5 工控系统行业漏洞统计

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，攻击者可利用漏洞获取敏感信息，使用解析代码中的错误来远程使调制解调器崩溃，导致远程权限提升等。

CNVD 收录的相关漏洞包括：Google Android 越界读取漏洞（CNVD-2022-53368、CNVD-2022-53384）、Google Android 缓冲区溢出漏洞（CNVD-2022-53367）、Google Android 越界写入漏洞（CNVD-2022-53369、CNVD-2022-53385）、Google Android 信息泄露漏洞（CNVD-2022-53372、CNVD-2022-53381、CNVD-2022-53380）。其中，“Google Android 越界读取漏洞（CNVD-2022-53368）、Google Android 缓冲区溢出漏洞（CNVD-2022-53367）、Google Android 越界写入漏洞（CNVD-2022-53369、CNVD-2022-53385）”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-2022-53368

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53367

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53369

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53372

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53381

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53380

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53384

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53385

2、 Cybozu 产品安全漏洞

Cybozu Garoon 是日本才望子（Cybozu）公司的一套门户型 OA 办公系统。该系统提供门户、E-mail、书签、日程安排、公告栏、文件管理等功能。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，禁用添加类别，更改数据，并在用户浏览器中在易受攻击的网站上下文中执行任意 HTML 和脚本代码等。

CNVD 收录的相关漏洞包括：Cybozu Garoon 授权问题漏洞（CNVD-2022-53804、CNVD-2022-54300、CNVD-2022-54304）、Cybozu Garoon 输入验证错误漏洞（CNVD-2022-53806、CNVD-2022-54301、CNVD-2022-54303）、Cybozu Garoon 操作限制绕过漏洞（CNVD-2022-54299）、Cybozu Garoon 跨站脚本漏洞（CNVD-2022-54343）。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-2022-53804
https://www.cnvd.org.cn/flaw/show/CNVD-2022-53806
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54299
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54301
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54300
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54303
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54304
https://www.cnvd.org.cn/flaw/show/CNVD-2022-54343

3、 Huawei 产品安全漏洞

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 是中国 Huawei 公司的一款基于 Android 开发的移动端操作系统。Honor Magic Ui 是中国 Honor 公司的一款基于 Android 开发的移动端操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，越界访问，进行拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 拒绝服务漏洞（CNVD-2022-53575、CNVD-2022-53574）、Huawei HarmonyOS 资源管理错误漏洞（CNVD-2022-53578、CNVD-2022-53579）、Huawei HarmonyOS 权限控制错误漏洞、Huawei HarmonyOS 拒绝服务漏洞（CNVD-2022-53576）、Huawei Emui 和 Honor Magic Ui 缓冲区溢出漏洞、Huawei EMUI 输入验证拒绝服务漏洞。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-2022-53575
https://www.cnvd.org.cn/flaw/show/CNVD-2022-53574
https://www.cnvd.org.cn/flaw/show/CNVD-2022-53578
https://www.cnvd.org.cn/flaw/show/CNVD-2022-53577

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53576

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53581

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53580

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53579

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，攻击者可利用漏洞通过多种协议访问网络破坏 MySQL Server，进而导致 MySQL Server 挂起或频繁重复崩溃（完全拒绝服务）。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2022-54312、CNVD-2022-54311、CNVD-2022-54310、CNVD-2022-54313、CNVD-2022-54315、CNVD-2022-54314、CNVD-2022-54317、CNVD-2022-54316）。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-2022-54312

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54311

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54310

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54313

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54315

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54314

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54317

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54316

5、Apache HTTP Server 输入验证错误漏洞

Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。本周，Apache HTTP Server 被披露存在输入验证错误漏洞，该漏洞源于对调用 r：parsebody(0)的 lua 脚本的恶意请求输入未能限制，攻击者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-2022-53584

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-2022-53545	LDAP Account Manager 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/LDAPAccountMa

			nager/lam/security/advisories/GHSA-q8g5-45m4-q95p
CNVD-2022-53560	TOTOLINK N600R 命令注入漏洞（CNVD-2022-53560）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://doudoudedi.github.io/2022/02/21/TOTOLINK-N600R-Command-Injection/
CNVD-2022-53585	Apache Maven 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：http://github.com/apache/maven-shared-utils/pull/40
CNVD-2022-54309	PortlandLabs Concrete Cms 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://documentation.concretecms.org/developers/introduction/version-history/910-release-notes
CNVD-2022-54329	Cisco Small Business 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rce-overflow-ygHByAK
CNVD-2022-54328	Microweber 跨站脚本漏洞（CNVD-2022-54328）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/microweber/microweber/commit/d28655183800b833abb20ccd55e1628f16ff65e4
CNVD-2022-54327	Cisco Small Business 缓冲区溢出漏洞（CNVD-2022-54327）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rce-overflow-ygHByAK
CNVD-2022-54363	WordPress HTML2WP plugin 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/c36d0ea8-bf5c-4af9-bd3d-911eb02adc14
CNVD-2022-53354	Online Car Wash Booking System SQL 注入漏洞（CNVD-2022-53354）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcecodester.com/php/15280/online-car-wash-booking-system-phpoop-free-source-code.html
CNVD-2022-54326	Cisco Small Business 缓冲区溢出漏洞（CNVD-2022-54326）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco

			-sa-sb-rv-rce-overflow-ygHByAK

小结：本周，Google 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，使用解析代码中的错误来远程使调制解调器崩溃，导致远程权限提升等。此外，Cybozu、Huawei、Oracle 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，禁用添加类别，更改数据，并在用户浏览器中在易受攻击的网站上下文中执行任意 HTML 和脚本代码，进行拒绝服务攻击等。另外，Apache HTTP Server 被披露存在输入验证错误漏洞，攻击者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、Rescue Dispatch Management System SQL 注入漏洞（CNVD-2022-53913）

验证描述

Rescue Dispatch Management System 是 Carlo Montero 个人开发者的一个救援调度管理系统。

Rescue Dispatch Management System v1.0 版本存在 SQL 注入漏洞，该漏洞源于/rdms/classes/Master.php?f=delete_report 页面缺少对外部输入 SQL 语句的验证，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/k0xx11/bug_report/blob/main/vendors/oretnom23/rescue-dispatch-management-system/SQL-1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-53913

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. 黑客利用 PrestaShop 零日漏洞入侵网店

PrestaShop 团队上周五发出紧急警告，有黑客正在针对使用 PrestaShop 平台的网站，利用以前未知的漏洞链进行代码执行，并很有可能在窃取客户的支付信息。该团队建议用户尽快对网站进行相关安全审查。

参考链接：https://www.freebuf.com/news/340135.html

2. Drupal 开发人员修复了 CMS 中的代码执行缺陷

Drupal 开发团队发布了安全更新来修复多个问题，包括一个任意 PHP 代码执行关键漏洞，被跟踪为 CVE-2022-25277。

参考链接：https://securityaffairs.co/wordpress/133625/security/drupal-flaws-2.html

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