国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 03 月 28 日-2022 年 04 月 03 日 **2022 年第 13 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 428 个，其中高危漏洞 153 个、中危漏洞 232 个、低危漏洞 43 个。漏洞平均分值为 6.06。本周收录的漏洞中，涉及 0day 漏洞 280 个（占 65%），其中互联网上出现“AppCMS 跨站脚本漏洞、Forkcms SQL 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 5300 个，与上周（4620 个）环比增加 15%。

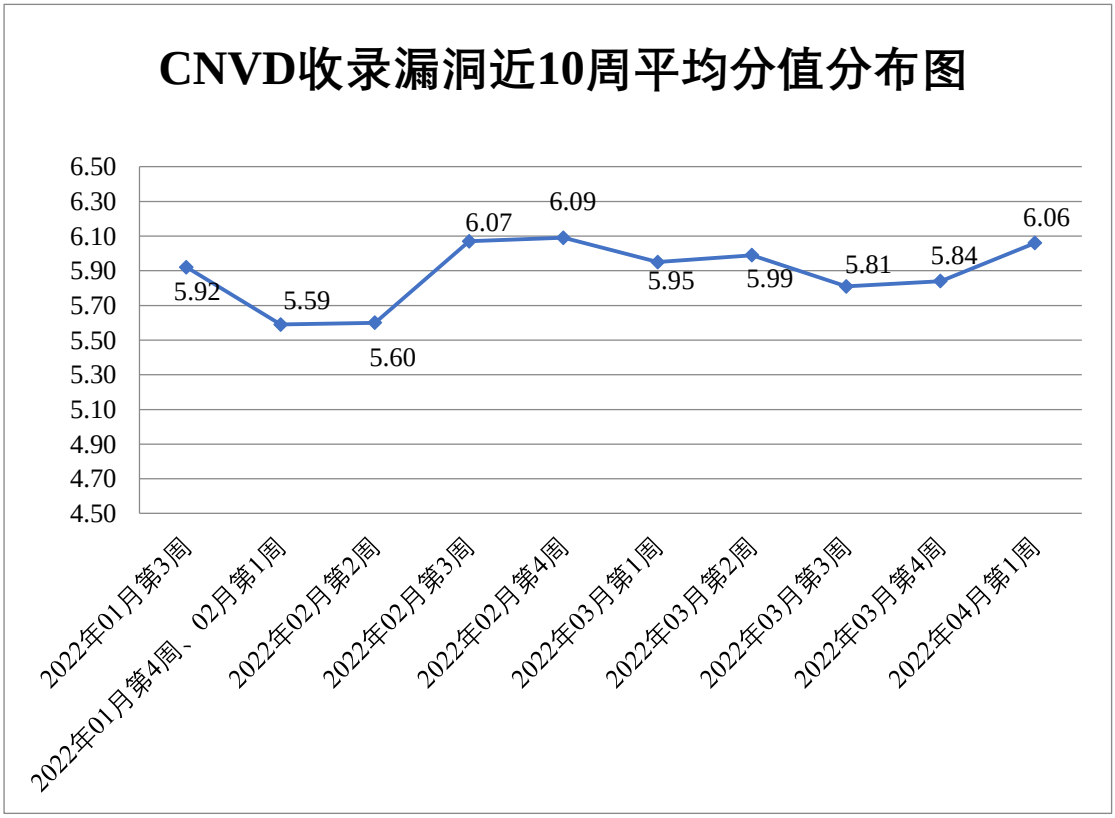

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 33 起，向基础电信企业通报漏洞事件 83 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 844 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 100 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 115 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：

珠海新华通软件股份有限公司、重庆梅安森科技股份有限公司、中新网络信息安全股份有限公司、中控泰科（北京）科技发展有限公司、浙江宇视科技有限公司、浙江三青环保科技有限公司、浙江标点信息科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、西门子（中国）有限公司、西安新软信息科技有限公司、西安佰联网络技术有限公司、武汉金同方科技有限公司、武汉烽火信息集成技术有限公司、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、潍坊雷鸣云网络科技有限公司、统信软件技术有限公司、台达电子企业管理（上海）有限公司、宿州市涛盛网络科技有限公司、苏州空谷网络科技有限公司、思科系统（中国）网络技术有限公司、视联动力信息技术股份有限公司、神州数码集团股份有限公司、深圳市锟铻科技有限公司、深圳市科迈爱康科技有限公司、深圳市嘉荣华科技有限公司、深圳市必联电子有限公司、深圳警翼智能科技股份有限公司、深圳奥联信息安全技术有限公司、上海美橙科技信息发展有限公司、上海金慧软件有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海二三四五移动科技有限公司、熵基科技股份有限公司、山东潍微科技股份有限公司、山东力创科技股份有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、日立产机系统（中国）有限公司、任子行网络技术股份有限公司、奇偶信息科技（上海）有限公司、普联技术有限公司、摩莎科技（上海）有限公司、励元科技（上海）有限公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、敬业钢铁有限公司、江西铭软科技有限公司、江苏天瑞仪器股份有限公司、济南爱程网络科技有限公司、吉翁电子（深圳）有限公司、华硕电脑（上海）有限公司、湖南云数信息科技有限公司、恒辉信达技术有限公司、河南吉海网络科技有限公司、合肥奇乐网络科技有限公司、杭州益仕行信息技术有限公司、杭州先锋电子技术股份有限公司、杭州图特信息科技有限公司、杭州七树科技有限公司、杭州海康威视数字技术股份有限公司、海南赞赞网络科技有限公司、哈尔滨伟成科技有限公司、广州唯众网络科技有限公司、广州青鹿教育科技有限公司、广州巨杉软件开发有限公司、高等教育出版社有限公司、东营金石软件有限公司、东方通科技股份有限公司、成都零起飞科技有限公司、常州科翔物联技术有限公司、北京云代账互联网科技有限公司、北京友邻电子商

务科技有限公司、北京医准智能科技有限公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京万维盈创科技发展有限公司、北京时空智友科技有限公司、北京清元优软科技有限公司、北京猎鹰安全科技有限公司、北京九思协同软件有限公司、北京火木科技有限公司、北京飞书科技有限公司、北京东方通科技股份有限公司、北京碧海威科技有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、安科瑞电气股份有限公司、安徽旭帆信息科技有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心、腾讯安全应急响应中心、站帮主 CMS、小说精品屋、TaoLer 社区系统、162100 网站、YAMAHA、voipmonitor、The Apache Software Foundation、taoCMS、SEACMS、Rockwell Automation、PiXORD Corporation、MongoDB、JreCms、emlog、Dreamer CMS、Brickcom、Axis Communications AB 和 Adobe。

本周，CNVD 发布了《关于 Spring 框架存在远程命令执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7541

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、北京华顺信安科技有限公司、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等单位报送公开收集的漏洞数量较多。亚信科技（成都）有限公司、山东云天安全技术有限公司、重庆都会信息科技、内蒙古洞明科技有限公司、杭州默安科技有限公司、北京山石网科信息技术有限公司、贵州泰若数字科技有限公司、江苏保旺达软件技术有限公司、长春嘉诚信息技术股份有限公司、山东新潮信息技术有限公司、武汉安域信息安全技术有限公司、河南信安世纪科技有限公司、海通证券股份有限公司、北京边界无限科技有限公司、上海纽盾科技股份有限公司、快页信息技术有限公司、河南灵创电子科技有限公司、深圳市魔方安全科技有限公司、河北华测信息技术有限公司、北京威努特技术有限公司、广州百蕴启辰科技有限公司、开元华创科技集团、南京禾盾信息科技有限公司、上海嘉韦思信息技术有限公司、武汉非尼克斯软件技术有限公司、河北千诚电子科技有限公司、厦门星舟科技有限公司、广州安亿信软件科技有限公司、北京远禾科技有限公司、思而听网络科技有限公司、麒麟软件有限公司、湖北珞格科技发展有限公司、浙江木链物联网科技有限公司、北方实验室（沈阳）股份有限公司、天空实验室、墨菲未来科技（北京）有限公司及其他个人白帽子向 CNVD 提交了 5300 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 2234 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

深信服科技股份有限公司	2118	0
上海交大	1190	1190
网神信息技术（北京）股份有限公司	527	527
上海斗象信息科技有限公司（漏洞盒子）	517	517
新华三技术有限公司	428	0
安天科技集团股份有限公司	259	0
西安四叶草信息技术有限公司	233	233
北京神州绿盟科技有限公司	162	5
北京数字观星科技有限公司	143	0
阿里云计算有限公司	132	0
杭州安恒信息技术股份有限公司	110	22
恒安嘉新（北京）科技股份公司	101	0
三六零数字安全科技集团有限公司	100	0
北京天融信网络安全技术有限公司	94	22
北京启明星辰信息安全技术有限公司	69	6
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	30	30
中国电信集团系统集成有限责任公司	30	0
远江盛邦（北京）网	21	21

络安全科技股份有限公司		
内蒙古云科数据服务股份有限公司	18	18
北京安信天行科技有限公司	13	13
京东科技信息技术有限公司	6	6
南京联成科技发展股份有限公司	3	3
北京智游网安科技有限公司	2	2
中兴通讯股份有限公司	2	2
北京华顺信安科技有限公司	323	0
亚信科技（成都）有限公司	105	0
山东云天安全技术有限公司	47	47
重庆都会信息科技	45	45
内蒙古洞明科技有限公司	44	44
杭州默安科技有限公司	41	41
北京山石网科信息技术有限公司	22	22
贵州泰若数字科技有限公司	20	20
江苏保旺达软件技术有限公司	18	18
杭州迪普科技股份有限公司	16	0
长春嘉诚信息技术股	14	14

份有限公司		
山东新潮信息技术有限公司	12	12
武汉安域信息安全技术有限公司	8	8
任子行网络技术股份有限公司	7	7
河南信安世纪科技有限公司	5	5
海通证券股份有限公司	4	4
北京边界无限科技有限公司	4	4
上海纽盾科技股份有限公司	4	4
快页信息技术有限公司	4	4
河南灵创电子科技有限公司	4	4
深圳市魔方安全科技有限公司	3	3
河北华测信息技术有限公司	3	3
北京威努特技术有限公司	2	2
广州百蕴启辰科技有限公司	2	2
开元华创科技集团	2	2
南京禾盾信息科技有限公司	1	1
上海嘉韦思信息技术有限公司	1	1
武汉非尼克斯软件技术有限公司	1	1

河北千诚电子科技有限公司	1	1
厦门星舟科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京远禾科技有限公司	1	1
思而听网络科技有限公司	1	1
麒麟软件有限公司	1	1
湖北珞格科技发展有限公司	1	1
浙江木链物联网科技有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
天空实验室	1	1
墨菲未来科技（北京）有限公司	1	1
个人	2354	2354
报送总计	9494	5300

本周漏洞按类型和厂商统计

本周，CNVD 收录了 428 个漏洞。WEB 应用 181 个，应用程序 118 个，网络设备（交换机、路由器等网络端设备）83 个，智能设备（物联网终端设备）16 个，操作系统 13 个，数据库 12 个，安全产品 5 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	181
应用程序	118
网络设备（交换机、路由器等网络端设备）	83
智能设备（物联网终端设备）	16
操作系统	13

数据库	12
安全产品	5

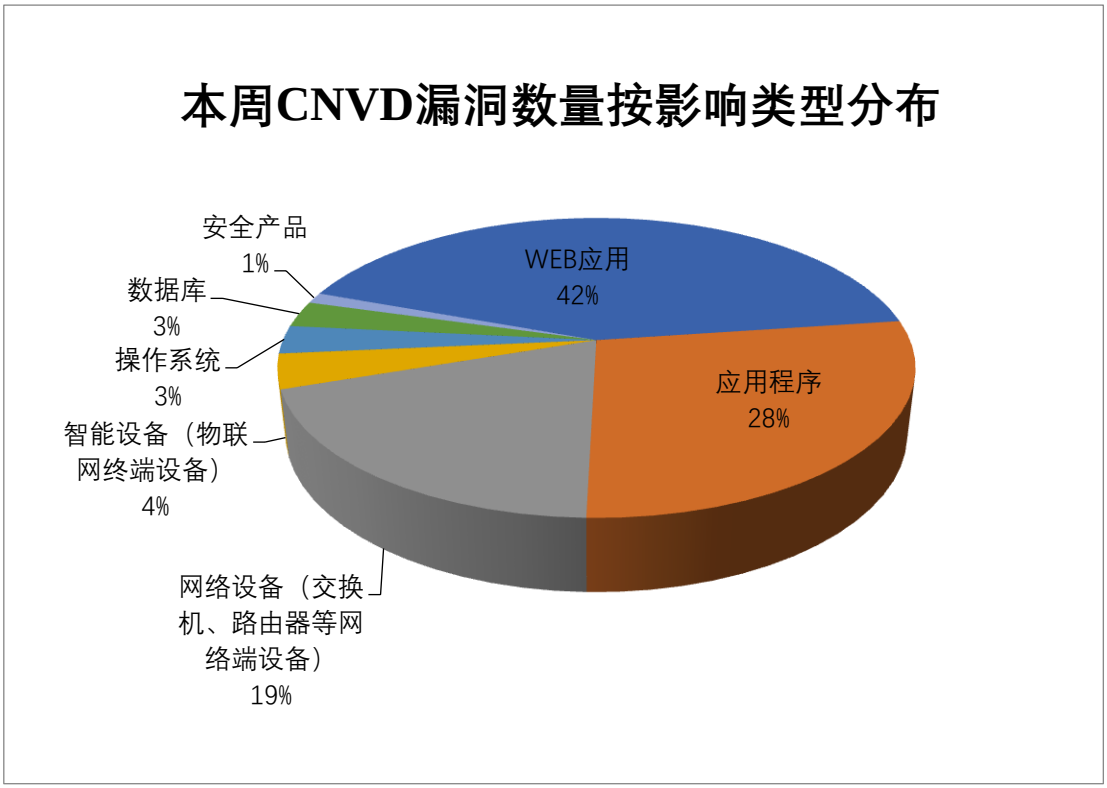

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、WordPress、Apple 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	Tenda	33	8%
2	WordPress	19	5%
3	Apple	17	4%
4	Microsoft	16	4%
5	Oracle	13	3%
6	北京星网锐捷网络技术有限公司	7	2%
7	Adobe	6	1%
8	GitLab	6	1%
9	深圳市必联电子有限公司	6	1%
10	其他	305	71%

本周行业漏洞收录情况

本周，CNVD 收录了 65 个电信行业漏洞，20 个移动互联网行业漏洞，2 个工控行

业漏洞（如下图所示）。其中，“Tenda AC6 SetIpMacBind 函数堆栈溢出漏洞、Tenda AC6 SetPptpServerCfg 函数堆栈溢出漏洞”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/

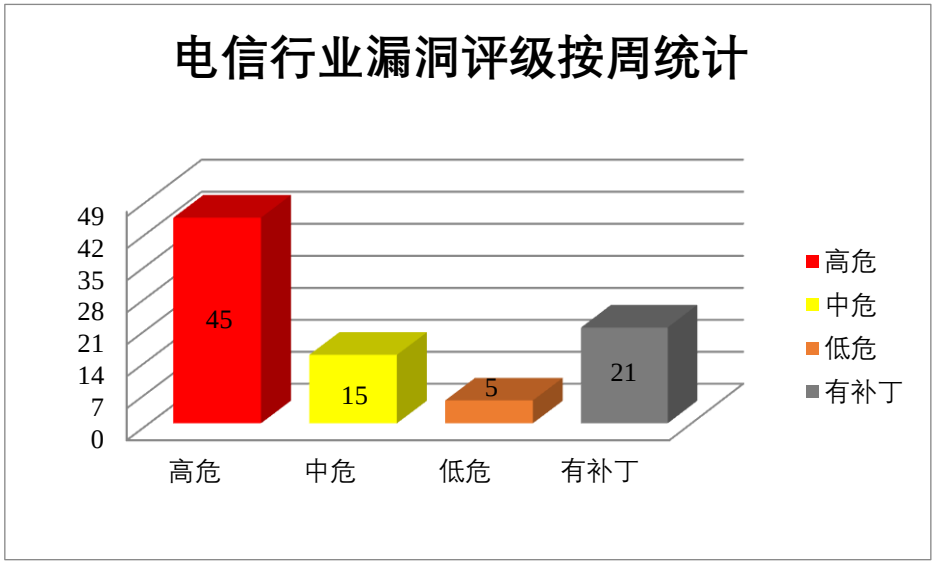

图 3 电信行业漏洞统计

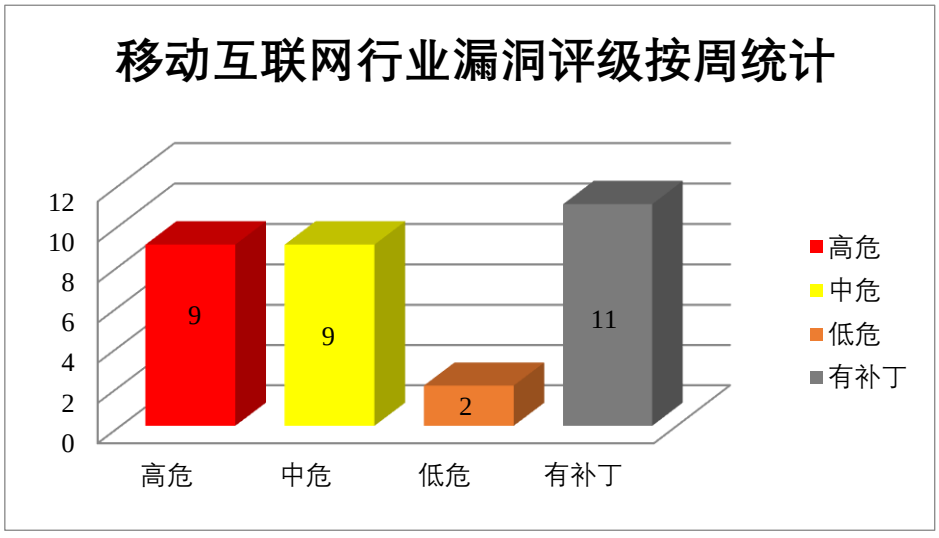

图 4 移动互联网行业漏洞统计

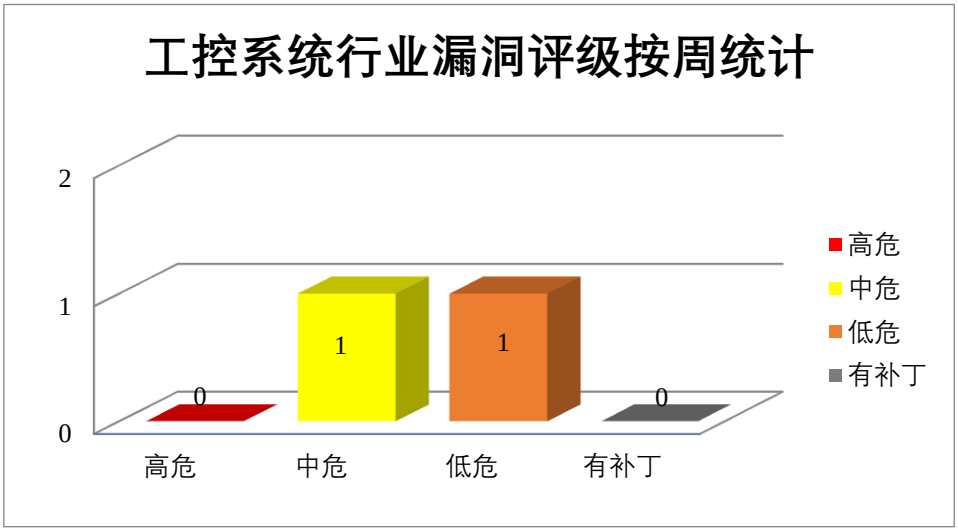

图 5 工控系统行业漏洞统计

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、 Tenda 产品安全漏洞

Tenda AC9 是中国腾达（Tenda）公司的一款无线路由器。Tenda AC6 是中国腾达（Tenda）公司的一款无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞破坏内存，或导致拒绝服务，任意命令执行等。

CNVD 收录的相关漏洞包括：Tenda AC6 堆栈溢出漏洞（CNVD-2022-23522）、Tenda AC6 openSchedWifi 函数堆栈溢出漏洞（CNVD-2022-23520、CNVD-2022-23521）、Tenda AC6 WifiBasicSet 函数堆栈溢出漏洞、Tenda AC9 Formsetqosband 函数堆栈溢出漏洞、Tenda AC9 openSchedWifi 函数堆栈溢出漏洞、Tenda AC9 saveparentcontrolinfo 函数堆栈溢出漏洞、Tenda AC9 saveparentcontrolinfo 函数缓冲区溢出漏洞。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-2022-23522

https://www.cnvd.org.cn/flaw/show/CNVD-2022-23521

https://www.cnvd.org.cn/flaw/show/CNVD-2022-23520

https://www.cnvd.org.cn/flaw/show/CNVD-2022-24425

https://www.cnvd.org.cn/flaw/show/CNVD-2022-24429

https://www.cnvd.org.cn/flaw/show/CNVD-2022-24428

https://www.cnvd.org.cn/flaw/show/CNVD-2022-24427

https://www.cnvd.org.cn/flaw/show/CNVD-2022-24426

2、 Apple 产品安全漏洞

Apple iOS 和 Apple iPadOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple watchOS 是一套智能手表操作系统。Apple tvOS 是美国苹果（Apple）公司的一套智能电视操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞获取敏感信息，通过 FaceTime 绕过已实施的安全限制实现共享敏感信息，在目标系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Apple iOS 和 Apple iPadOS 释放后重用漏洞、多款 Apple 产品越界读取漏洞（CNVD-2022-23002）、多款 Apple 产品释放后重用漏洞、Apple iOS 和 Apple iPadOS 输入验证错误漏洞、多款 Apple 产品缓冲区溢出漏洞（CNVD-2022-23007、CNVD-2022-23006）、Apple iOS、Apple iPadOS 和 Apple tvOS 缓冲区溢出漏洞、Apple iOS、iPadOS 和 macOS Monterey 权限许可和访问控制问题漏洞。其中，“Apple iOS 和 Apple iPadOS 释放后重用漏洞、多款 Apple 产品释放后重用漏洞、多款 Apple 产品缓冲区溢出漏洞（CNVD-2022-23007）、Apple iOS、Apple iPadOS 和 Apple tvOS 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-2022-23003
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23002
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23001
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23000
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23007
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23006
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23005
https://www.cnvd.org.cn/flaw/show/CNVD-2022-23004

3、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。Oracle Taleo 是美国甲骨文（Oracle）公司的一个强大的独立人才招聘套件。用于寻找和聘用最佳候选人。Oracle WebLogic Server 是美国甲骨文（Oracle）公司的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞破坏或删除数据，在系统上执行远程代码或导致拒绝服务(部分 DOS)等。

CNVD 收录的相关漏洞包括：Oracle MySQL 输入验证错误漏洞（CNVD-2022-25200、CNVD-2022-25201、CNVD-2022-25199、CNVD-2022-25198）、Oracle MySQL 缓冲区溢出漏洞（CNVD-2022-25202）、Oracle Taleo 拒绝服务漏洞、Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-25228、CNVD-2022-25227）。其中，“Oracle

Taleo 拒绝服务漏洞”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-2022-25199
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25198
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25202
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25201
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25200
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25212
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25228
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25227

4、 WordPress 产品安全漏洞

WordPress 是 Wordpress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress plugin 是 WordPress 开源的一个应用插件。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未授权访问，在客户端执行 JavaScript 代码，执行非法 SQL 命令窃取数据库敏感数据等。

CNVD 收录的相关漏洞包括：WordPress WP Email Users plugin SQL 注入漏洞、WordPress WP Voting Contest plugin 跨站脚本漏洞、WordPress Team Circle Image Slider With Lightbox plugin 跨站脚本漏洞、WordPress WooCommerce plugin SQL 注入漏洞、WordPress Photo Gallery by 10Web plugin SQL 注入漏洞、WordPress Simple Quotation plugin 跨站脚本漏洞、WordPress Page Builder KingComposer plugin 访问控制错误错误漏洞、WordPress Multisite Content Copier/Updater plugin 跨站脚本漏洞。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-2022-25754
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25753
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25756
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25755
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25758
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25757
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25759
https://www.cnvd.org.cn/flaw/show/CNVD-2022-25760

5、Tenda AC6 堆栈溢出漏洞

Tenda AC6 是一款无线路由器。本周，Tenda AC6 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞破坏内存，或导致拒绝服务。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.cnv

d.org.cn/flaw/show/CNVD-2022-23523

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-2022-23459	Tianocore Edk2 缓冲区溢出漏洞（CNVD-2022-23459）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.tianocore.org/show_bug.cgi?id=3360
CNVD-2022-23458	Wordline HIDCCEMonitorSVC 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://hansesecure.de/2021/12/vulnerability-wordline/?lang=en
CNVD-2022-23462	VMware Tools for Windows 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2022-0007.html
CNVD-2022-23461	Hazelcast 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/hazelcast/hazelcast/commit/4d6b666cd0291abd618c3b95cdbb51aa4208e748
CNVD-2022-23460	Tianocore Edk2 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.tianocore.org/show_bug.cgi?id=3387
CNVD-2022-23470	cmark-gfm 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://github.com/github/cmark-gfm/security/advisories/GHSA-mc3g-88wq-6f4x
CNVD-2022-23471	Microsoft Dynamics 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23272
CNVD-2022-23474	Microsoft Roaming Security Rights Management Services 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21974
CNVD-2022-23485	Pytorch-Lightning 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/pytorchlightning/pytorch-lightning/commit/8b7a12c52e52a06408e9231647839ddb4665e8ae

CNVD-2022-23489	nbd 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://sourceforge.net/projects/nbd/files/nbd/

小结：本周，Tenda 产品被披露存在多个漏洞，攻击者可利用漏洞破坏内存，或导致拒绝服务，任意命令执行等。此外，Apple、Oracle、WordPress 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，通过 FaceTime 绕过已实施的安全限制实现共享敏感信息，在目标系统上执行任意代码等。另外，Tenda AC6 被披露存在堆栈溢出漏洞，攻击者可利用该漏洞破坏内存，或导致拒绝服务。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、AppCMS 跨站脚本漏洞

验证描述

AppCMS 是一款用于移动应用程序下载的内容管理系统（CMS）。

AppCMS2.0.101 版本中的 upload/callback.php 文件存在跨站脚本漏洞。远程攻击者可借助‘params’参数利用该漏洞注入任意的 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/source-trace/appcms/issues/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-25773

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. 苹果发布紧急补丁以修复被积极利用的零日漏洞

苹果发布了一个紧急安全补丁，以解决两项被积极利用以入侵 iPhone、iPad 和 Mac 的零日漏洞，并建议用户尽快安装安全更新。

参考链接：https://securityaffairs.co/wordpress/129672/security/apple-emergency-patches-zero-days.html

2. 美国国务院完成 370 亿美元的预算申请为网络空间和数字政策局增员

5 日起，美国国务院将为其网络空间和数字政策局配备多达 100 名新人员。网络局

将重点提高对网络外交的认识，以应对勒索软件攻击、关键网络基础设施攻击等。

参考链接：https://www.cnbeta.com/articles/tech/1254583.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