# 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 18 日-2022 年 07 月 24 日** **2022 年第 29 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 347 个，其中高危漏洞 130 个、中危漏洞 180 个、低危漏洞 37 个。漏洞平均分值为 6.16。本周收录的漏洞中，涉及 0day 漏洞 280 个（占 81%），其中互联网上出现“Tenda M3 formSetStoreWeb 函数缓冲区溢出漏洞、Taocms SQL 注入漏洞（CNVD-2022-53257）”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 10876 个，与上周（6909 个）环比增加 57%。

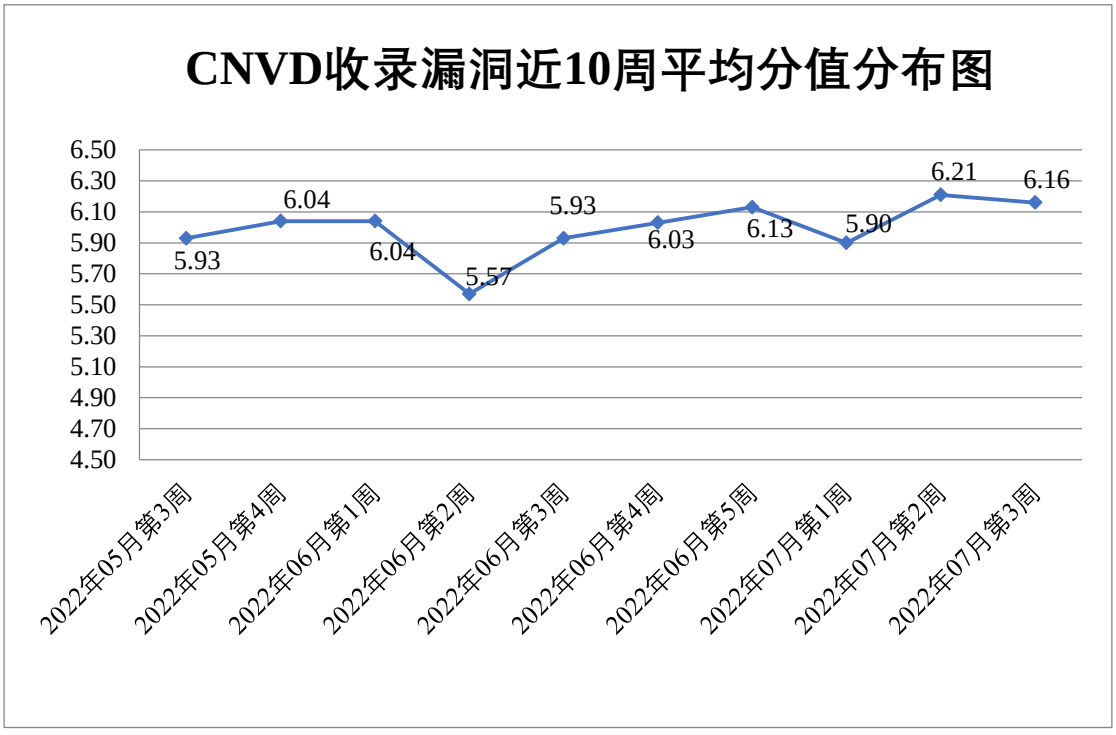


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 40 起，向基础电信企业通报漏洞事件 13 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 1367 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 190 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：

深圳市网域科技技术有限公司、深圳市前海欢雀科技有限公司、深圳市农博创新科技有限公司、深圳市尼高企业形象设计有限公司、深圳市脸萌科技有限公司、深圳市蓝凌软件股份有限公司、深圳市聚网捷科技有限公司、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、申瓯通信设备有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海军慧医疗管理有限公司、上海金电网安科技有限公司、上海货鸟网络科技有限公司、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、上海布雷德科技有限公司、厦门圆古网络科技有限公司、厦门网中网软件有限公司、厦门市灵鹿谷科技有限公司、普联技术有限公司、宁夏链点互联网医院有限公司、朗坤智慧科技股份有限公司、江苏天瑞仪器股份有限公司、货披发（厦门）信息科技有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南美食流智能科技有限公司、恒锋信息科技股份有限公司、河南可中信息技术有限公司、河北蓝蜂信息科技有限公司、河北华厚天成环保技术有限公司、杭州雄伟科技开发股份有限公司、杭州吾游吾旅信息科技有限公司、杭州瑞成信息技术有限公司、杭州九麒科技有限公司、杭州今奥信息科技股份有限公司、杭州宏服软件有限公司、杭州合言信息科技有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、杭州灿越网络科技股份有限公司、广州网易计算机系统有限公司、广州快塑电子商务有限公司、广东天宸网络科技有限公司、富士施乐（中国）有限公司、东华软件股份公司、东莞市通天星软件科技有限公司、德施曼机电（中国）有限公司、成都智一云科科技有限公司、成都青软青之软件有限公司、北京字节跳动科技有限公司、北京卓易讯畅科技有限公司、北京中科华博科技有限公司、北京致远互联软件股份有限公司、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、北京小米科技有限责任公司、北京网御星云信息技术有限公司、北京网医联盟科技有限公司、北京平凯星辰科技发展有限公司、北京猎鹰安全科技有限公司、北京快手科技有限公司、北京九思协同软件有限公司、北京竞业达数码科技股份有限公司、北京华夏创新科技有限公司、北京国栋科技有限公司、北京点为信息科技有限公司、北京棣南新宇科技有限公司、北京邦永科技有限公司、北京百卓网络技术有限公司、北京安盟信息技术股份有限公司、北京安博通科技股份有限公司、北京爱奇艺科技有限公司、腾讯安全应急响应中心、美团安全应急响应中心、熊海 CMS、若依、狂雨小说 cms、webcamx、UCMS、TRENDnet、

seacms、Python Software Foundation、PortSwigger、PHPGurukul、Percona LLC.、NETGEAR、Kong Inc.、Grafana Labs、Cypress Solutions Inc.、ChurchCRM、Cambium Networks 和 Belkin International,Inc。

本周，CNVD 发布了《Oracle 发布 2022 年 7 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7916

## 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、北京数字观星科技有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、贵州泰若数字科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州迪普科技股份有限公司、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、苏州棱镜七彩信息科技有限公司、河南灵创电子科技有限公司、平安银河实验室、北京远禾科技有限公司、山石网科通信技术股份有限公司、统信软件技术有限公司、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攻防实验室、快页信息技术有限公司、山东新潮信息技术有限公司、北京冠程科技有限公司、广州易东信息安全技术有限公司、上海纽盾科技股份有限公司、任子行网络技术股份有限公司、墨菲未来科技（北京）有限公司、广东唯顶信息科技股份有限公司、河南信安世纪科技有限公司、北京安盟信息技术股份有限公司、长春嘉诚信息技术股份有限公司、浙江安腾信息技术有限公司、南京深安科技有限公司、思而听网络科技有限公司、上海观安信息技术股份有限公司、广电奇安网络科技（重庆）有限公司、福建省海峡信息技术有限公司、江苏耘和计算机系统工程有限公司、华堡天建（天津）信息技术有限公司、腾讯安全天马实验室、博智安全科技股份有限公司、河北千诚电子科技有限公司、江西和尔惠信息技术有限公司、北京东方通科技股份有限公司、北京升鑫网络科技有限公司、北京华云安信息技术有限公司、广州安亿信软件科技有限公司及其他个人白帽子向 CNVD 提交了 10876 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、奇安信网神（补天平台）和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 8920 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） | 3510 | 3510 |
| 奇安信网神（补天平台） | 3414 | 3414 |

| | | |
|---|---|---|
| 三六零数字安全科技集团有限公司 | 1208 | 1208 |
| 上海交大 | 788 | 788 |
| 深信服科技股份有限公司 | 513 | 2 |
| 北京神州绿盟科技有限公司 | 396 | 2 |
| 新华三技术有限公司 | 385 | 0 |
| 北京数字观星科技有限公司 | 311 | 0 |
| 北京天融信网络安全技术有限公司 | 238 | 25 |
| 杭州安恒信息技术股份有限公司 | 219 | 112 |
| 安天科技集团股份有限公司 | 217 | 0 |
| 恒安嘉新（北京）科技股份公司 | 101 | 0 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 75 | 75 |
| 北京启明星辰信息安全技术有限公司 | 68 | 12 |
| 天津市国瑞数码安全系统股份有限公司 | 60 | 0 |
| 京东科技信息技术有限公司 | 47 | 23 |
| 南京众智维信息科技有限公司 | 36 | 36 |
| 中国电信集团系统集成有限责任公司 | 21 | 0 |
| 西安四叶草信息技术有限公司 | 17 | 17 |
| 北京知道创宇信息技术有限公司 | 14 | 0 |

| | | |
|---|---|---|
| 内蒙古奥创科技有限公司 | 5 | 5 |
| 北京长亭科技有限公司 | 3 | 3 |
| 北京知道创宇信息技术有限公司 | 3 | 0 |
| 北京华顺信安科技有限公司 | 309 | 3 |
| 贵州泰若数字科技有限公司 | 88 | 88 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 53 | 53 |
| 杭州迪普科技股份有限公司 | 26 | 1 |
| 河南东方云盾信息技术有限公司 | 18 | 18 |
| 北京山石网科信息技术有限公司 | 11 | 11 |
| 苏州棱镜七彩信息科技有限公司 | 6 | 6 |
| 河南灵创电子科技有限公司 | 6 | 6 |
| 平安银河实验室 | 5 | 5 |
| 北京远禾科技有限公司 | 5 | 5 |
| 山石网科通信技术股份有限公司 | 5 | 5 |
| 统信软件技术有限公司 | 5 | 5 |
| 浙江木链物联网科技有限公司 | 5 | 5 |
| 中能融合智慧科技有限公司攻防实验室 | 4 | 4 |
| 快页信息技术有限公 | 4 | 4 |

| | | |
|---|---|---|
| 司 | | |
| 山东新潮信息技术有限公司 | 4 | 4 |
| 北京冠程科技有限公司 | 4 | 4 |
| 广州易东信息安全技术有限公司 | 4 | 4 |
| 上海纽盾科技股份有限公司 | 3 | 3 |
| 任子行网络技术股份有限公司 | 3 | 3 |
| 墨菲未来科技（北京）有限公司 | 3 | 3 |
| 广东唯顶信息科技股份有限公司 | 2 | 2 |
| 河南信安世纪科技有限公司 | 2 | 2 |
| 北京安盟信息技术股份有限公司 | 2 | 2 |
| 长春嘉诚信息技术股份有限公司 | 2 | 2 |
| 浙江安腾信息技术有限公司 | 1 | 1 |
| 南京深安科技有限公司 | 1 | 1 |
| 思而听网络科技有限公司 | 1 | 1 |
| 上海观安信息技术股份有限公司 | 1 | 1 |
| 广电奇安网络科技（重庆）有限公司 | 1 | 1 |
| 福建省海峡信息技术有限公司 | 1 | 1 |
| 江苏耘和计算机系统工程有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 华堡天建（天津）信息技术有限公司 | 1 | 1 |
| 腾讯安全天马实验室 | 1 | 1 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 河北千诚电子科技有限公司 | 1 | 1 |
| 江西和尔惠信息技术有限公司 | 1 | 1 |
| 北京东方通科技股份有限公司 | 1 | 1 |
| 北京升鑫网络科技有限公司 | 1 | 1 |
| 北京华云安信息技术有限公司 | 1 | 1 |
| 广州安亿信软件科技有限公司 | 1 | 1 |
| CNCERT 浙江分中心 | 5 | 5 |
| CNCERT 贵州分中心 | 5 | 5 |
| CNCERT 四川分中心 | 2 | 2 |
| CNCERT 内蒙古分中心 | 2 | 2 |
| 个人 | 1366 | 1366 |
| 报送总计 | 13624 | 10876 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 347 个漏洞。WEB 应用 138 个，网络设备（交换机、路由器等网络端设备）76 个，应用程序 63 个，操作系统 38 个，智能设备（物联网终端设备）24 个，数据库 7 个，安全产品 1 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 | 138 |
| 网络设备（交换机、路由器等网络端设备） | 76 |
| 应用程序 | 63 |

| | |
|---|---|
| 操作系统 | 38 |
| 智能设备（物联网终端设备） | 24 |
| 数据库 | 7 |
| 安全产品 | 1 |

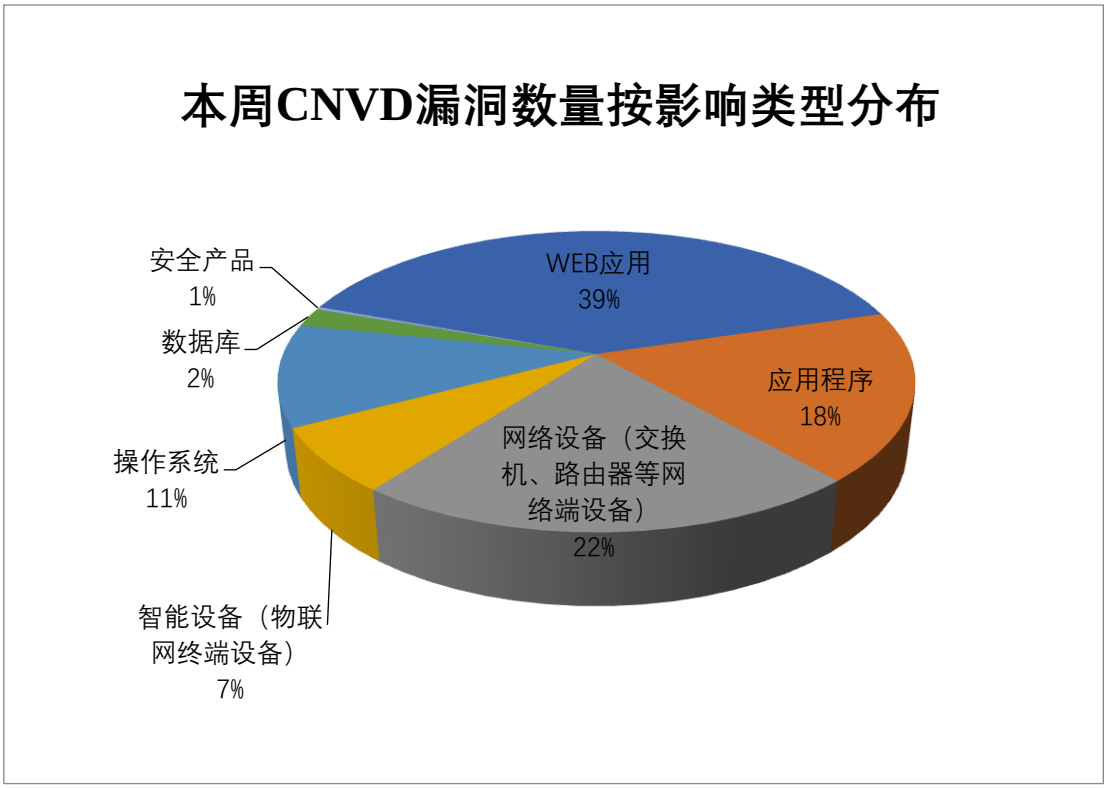


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、新华三技术有限公司、Oracle 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 | Google | 17 | 5% |
| 2 | 新华三技术有限公司 | 16 | 5% |
| 3 | Oracle | 13 | 4% |
| 4 | H3C | 12 | 3% |
| 5 | Huawei | 12 | 3% |
| 6 | HP | 11 | 3% |
| 7 | GNU | 11 | 3% |
| 8 | Adobe | 9 | 3% |
| 9 | PHPList | 8 | 2% |
| 10 | 其他 | 238 | 69% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 57 个电信行业漏洞，28 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Google Android 资源管理错误漏洞（CNVD-2022-52275）、Google Android 任意代码执行漏洞”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/

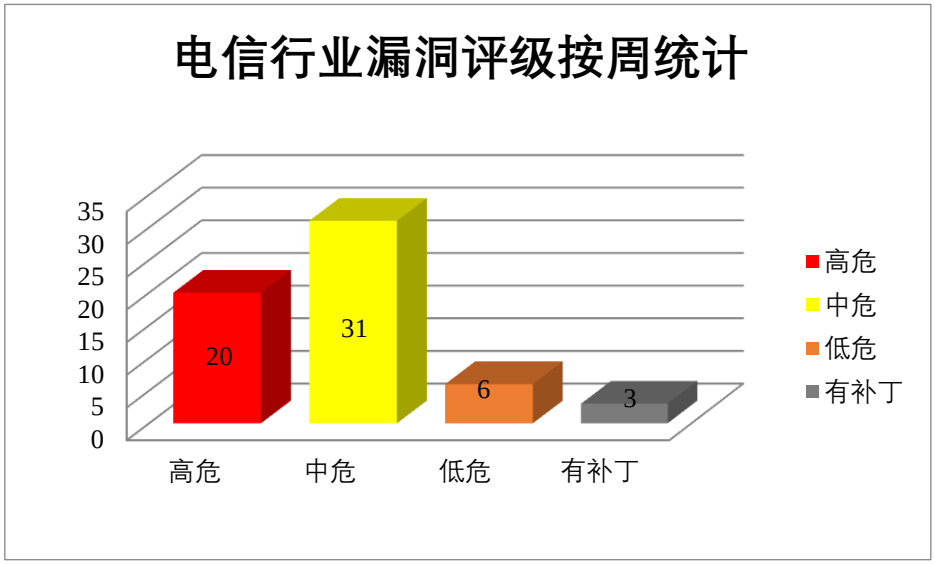


图 3 电信行业漏洞统计

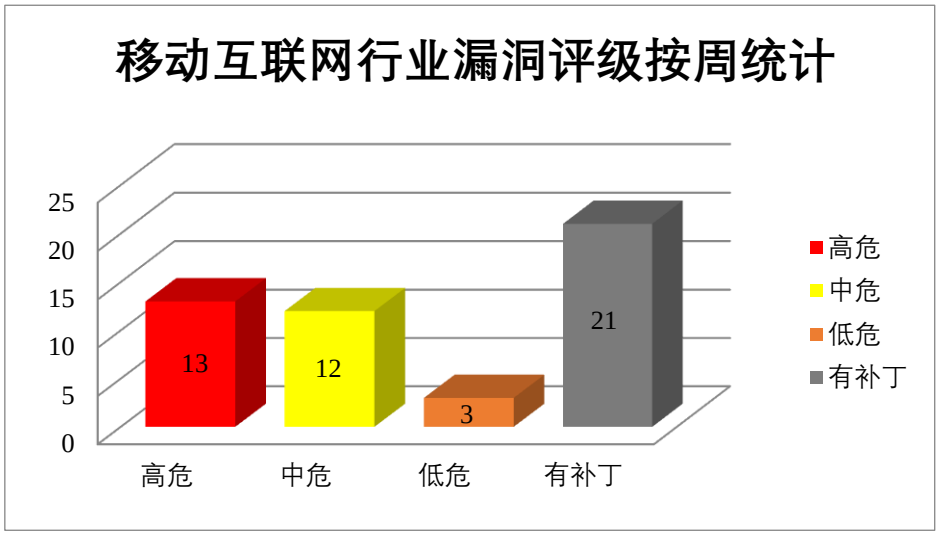


图 4 移动互联网行业漏洞统计

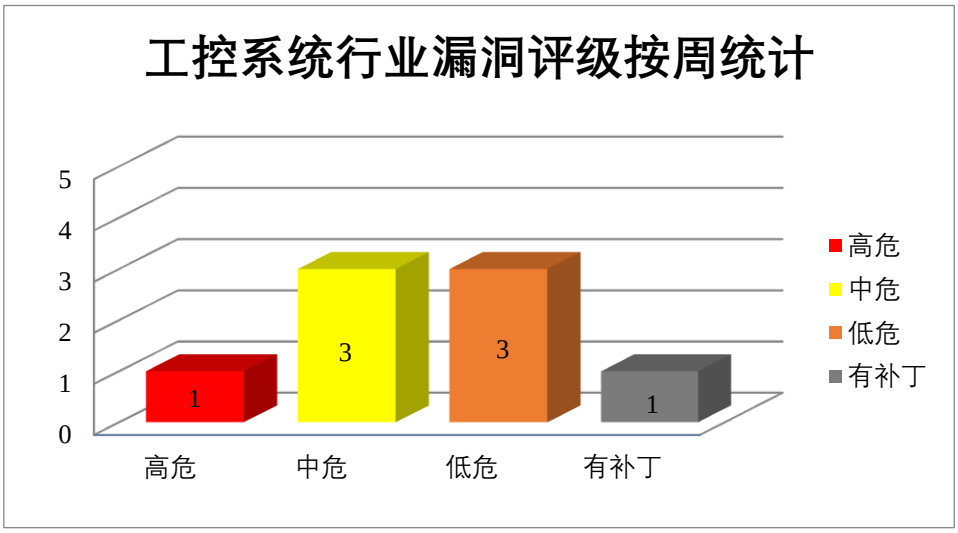


图 5 工控系统行业漏洞统计

## 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 Character Animator 是美国奥多比（Adobe）公司的一款动作捕捉和动画制作工具。Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe Media Encoder 是美国奥多比（Adobe）公司的一款音、视频编码应用程序。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。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敏感内存泄露，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Character Animator 越界写入漏洞、Adobe Photoshop 越界写入漏洞（CNVD-2022-52087）、Adobe Media Encoder 内存破坏漏洞（CNVD-2022-52098）、多款 Adobe 资源管理错误漏洞（CNVD-2022-52291）、多款 Adobe 产品缓冲区溢出漏洞（CNVD-2022-52922）、多款 Adobe 产品越界写入漏洞（CNVD-2022-52921）、多款 Adobe 产品资源管理错误漏洞（CNVD-2022-52920）、多款 Adobe 产品越界读取漏洞（CNVD-2022-52924）。其中，除“多款 Adobe 产品越界读取漏洞（CNVD-2022-52924）”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-2022-52081

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52087

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52098

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52291

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52922

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52921

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52920

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52924

### 2、Huawei 产品安全漏洞

Huawei MindSpore Community 是中国华为（Huawei）公司的开源深度学习框架。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 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。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，攻击者可利用漏洞获取敏感信息，导致设备崩溃等。

CNVD 收录的相关漏洞包括：Huawei MindSpore Community SparseToDense 信息泄露漏洞、Huawei MindSpore Community Transpose 信息泄露漏洞、HUAWEI EMUI 信息泄露漏洞、HUAWEI HarmonyOS 缓冲区溢出漏洞（CNVD-2022-52823）、HUAWEI HarmonyOS 拒绝服务漏洞、HUAWEI HarmonyOS 安全模块授权问题漏洞、HUAWEI HarmonyOS SystemUI 模块权限管理漏洞、Huawei Emui 和 Honor Magic Ui 缓冲区溢出漏洞（CNVD-2022-52826）。其中，“HUAWEI HarmonyOS 拒绝服务漏洞、Huawei Emui 和 Honor Magic Ui 缓冲区溢出漏洞（CNVD-2022-52826）”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-2022-52099

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52100

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52818

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52823

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52822

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52821

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52820

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52826

### 3、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 权限提升漏洞（CNVD-2022-52264、CNVD-2022-52265、CNVD-2022-52268、CNVD-2022-52267、CNVD-2022-52271、CNVD-2022-52270）、Google Android 缓冲区溢出漏洞（CNVD-2022-52274）、Google Android 输入验证错误漏洞（CNVD-2022-52273）。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-2022-52264
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52265
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52268
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52267
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52271
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52270
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52274
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52273

### 4、Oracle 产品安全漏洞

Oracle PeopleSoft Enterprise PRTL Interaction Hub 是美国甲骨文（Oracle）公司的一个企业门户交互中心组件。Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Oracle Access Manager 是美国甲骨文（Oracle）公司的提供创新的新服务来补充传统的访问管理功能。Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。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，导致拒绝服务，执行任意代码等。

CNVD 收录的相关漏洞包括：Oracle MySQL 输入验证错误漏洞（CNVD-2022-52562）、Oracle PeopleSoft Enterprise PRTL Interaction Hub 访问控制错误漏洞、Oracle Fusion Middleware Helidon 输入验证错误漏洞、Oracle Access Manager 存在输入验证错误漏洞、Oracle Database Server 输入验证错误漏洞（CNVD-2022-52564）、Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-52566）、Oracle MySQL 输入验证错误漏洞（CNVD-2022-53246、CNVD-2022-53249）。其中“Oracle WebLogic Server 存在拒绝服务漏洞、Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-52566）、Oracle MySQL 输入验证错误漏洞（CNVD-2022-53246）”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-2022-52562
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52561
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52560
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52565
https://www.cnvd.org.cn/flaw/show/CNVD-2022-52564

https://www.cnvd.org.cn/flaw/show/CNVD-2022-52566

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53246

https://www.cnvd.org.cn/flaw/show/CNVD-2022-53249

### 5、Juniper Networks Junos OS 输入验证错误漏洞（CNVD-2022-53250）

Juniper Networks Junos OS 是美国瞻博网络（Juniper Networks）公司的一套专用于该公司的硬件设备的网络操作系统。该操作系统提供了安全编程接口和 Junos SDK。本周，Juniper Networks Junos OS 被披露存在输入验证错误漏洞。攻击者利用该漏洞通过 MPLS IPv6 Packet 引起 Jonos OS 的致命错误导致其拒绝服务。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-2022-53250

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-2022-52290 | GLPI SQL 注入漏洞（CNVD-2022-52290） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/glpi-project/glpi/security/advisories/GHSA-w2gc-v2gm-q7wq |
| CNVD-2022-52835 | Apache Spark 命令注入漏洞 | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：https://spark.apache.org/security.html |
| CNVD-2022-53001 | phplist SQL 注入漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://seclists.org/fulldisclosure/2017/Mar/45 |
| CNVD-2022-52999 | phplist SQL 注入漏洞（CNVD-2022-52999） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://seclists.org/fulldisclosure/2017/Mar/45 |
| CNVD-2022-52081 | Adobe Character Animator 越界写入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/character_animator/apsb22-21.html |
| CNVD-2022-52087 | Adobe Photoshop 越界写入漏洞（CNVD-2022-52087） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/photoshop/apsb22-20.html |
| CNVD-2022 | Adobe Media Encoder 内存 | 高 | 用户可参考如下供应商提供的安全 |

| | | | |
|---|---|---|---|
| -52098 | 破坏漏洞（CNVD-2022-52098） | | 公告获得补丁信息：https://helpx.adobe.com/security/products/media-encoder/apsb21-118.html |
| CNVD-2022-52264 | Google Android 权限提升漏洞（CNVD-2022-52264） | 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/2022-06-01 |
| CNVD-2022-52274 | Google Android 缓冲区溢出漏洞（CNVD-2022-52274） | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：https://source.android.com/security/bulletin/2022-06-01 |
| CNVD-2022-53246 | Oracle MySQL 输入验证错误漏洞（CNVD-2022-53246） | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：https://www.oracle.com/security-alerts/cpujul2022.html |

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞导致敏感内存泄露，在当前用户的上下文中执行任意代码等。此外，Huawei、Google、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，导致设备崩溃，执行任意代码等。另外，Juniper Networks Junos OS 被披露存在输入验证错误漏洞。攻击者可利用漏洞通过 MPLS IPv6 Packet 引起 Jonos OS 的致命错误导致其拒绝服务。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、Tenda M3 formSetStoreWeb 函数缓冲区溢出漏洞

**验证描述**

Tenda M3 是中国腾达（Tenda）公司的一款门禁控制器。

Tenda M3 V1.0.0.12 版本存在缓冲区溢出漏洞，该漏洞源于 formSetStoreWeb 函数的 ssidList, storeName, trademark 参数对输入数据不检查其长度。攻击者可利用该漏洞导致拒绝服务攻击。

**验证信息**

POC 链接：https://github.com/d1tto/IoT-vuln/tree/main/Tenda/M3/formSetStoreWeb

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-52124

**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. Atlassian 修复了一个关键的 Confluence 漏洞

Atlassian 发布了安全更新，以解决影响 Confluence Server 和 Confluence Data Center 的安全漏洞。

参考链接：https://securityaffairs.co/wordpress/133496/hacking/atlassian-confluence-server-data-center-flaw.html

### 2. Apple 修复了 iOS、iPadOS、macOS、tvOS 和 watchOS 设备中的多个缺陷

Apple 发布了安全更新，以解决影响 iOS、iPadOS、macOS、tvOS 和 watchOS 设备的多个漏洞。

参考链接：https://securityaffairs.co/wordpress/133486/security/apple-security-updates.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