# 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 05 日-2022 年 09 月 11 日** **2022 年第 36 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 320 个，其中高危漏洞 117 个、中危漏洞 166 个、低危漏洞 37 个。漏洞平均分值为 6.14。本周收录的漏洞中，涉及 0day 漏洞 206 个（占 64%），其中互联网上出现“Contec SolarView Compact 远程代码执行漏洞、Swftools 缓冲区溢出漏洞（CNVD-2022-62209）”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 7225 个，与上周（8944 个）环比减少 19%。

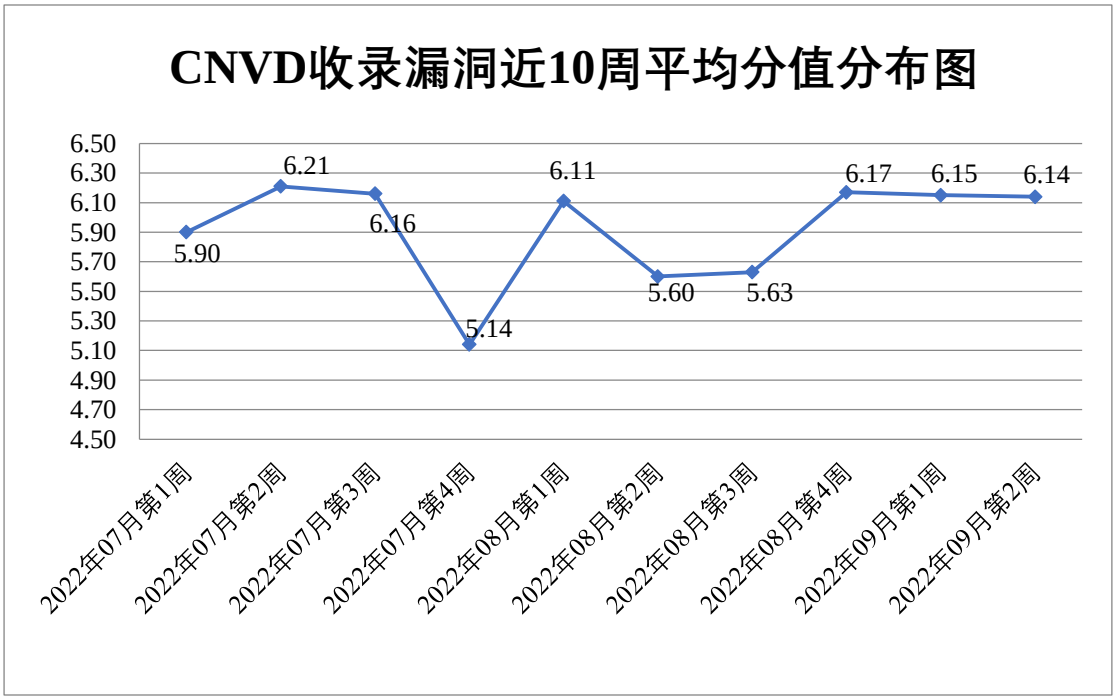


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 23 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 270 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 22 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 104 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：

郑州卡卡罗特软件科技有限公司、浙江大华技术股份有限公司、长沙立语信息科技有限公司、云易宿（北京）文旅科技有限公司、云南链滴科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、武汉神州数码云科网络技术有限公司、武汉达梦数据库股份有限公司、深圳市美科星通信技术有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳极速创想科技有限公司、上海茸易科技有限公司、上海华测导航技术股份有限公司、上海海典软件股份有限公司、上海亘岩网络科技有限公司、上海斐讯数据通信技术有限公司、山东云则信息技术有限公司、山东万岳信息科技有限公司、厦门四信通信科技有限公司、普联技术有限公司、迈普通信技术股份有限公司、零视技术（上海）有限公司、乐星电气（无锡）有限公司、金蝶国际软件集团有限公司、江阴互盛网络科技有限公司、江西怡杉环保股份有限公司、济南时空超越科技有限公司、华硕电脑（上海）有限公司、湖南壹拾捌号网络技术有限公司、弘扬软件股份有限公司、杭州金安易软件有限公司、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、广州友财信息科技有限公司、广州齐博网络科技有限公司、广州红帆科技有限公司、广州鼎成信息科技有限公司、广东飞企互联科技股份有限公司、畅捷通信息技术股份有限公司、布丁酒店浙江股份有限公司、北京中航讯科技股份有限公司、北京万学教育科技有限公司、北京数字政通科技股份有限公司、北京猎鹰安全科技有限公司、北京国信冠群技术有限公司、北京国炬信息技术有限公司、北京东方通科技股份有限公司、北京辰安科技股份有限公司、北京北科驿唐科技有限公司、北京宝兰德软件股份有限公司和北京百卓网络技术有限公司。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、深信服科技股份有限公司、新华三技术有限公司、北京数字观星科技有限公司、安天科技集团股份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、河南信安世纪科技有限公司、重庆都会信息科技有限公司、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、北京山石网科信息技术有限公司、河南灵创电子科技有限公司、长春嘉诚信息技术股份有限公司、北京升鑫网络科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、中能融合智慧科技有限公司攻防实验室、江苏省信息安

全测评中心、快页信息技术有限公司、联通沃悦读科技文化有限公司、北京君云天下科技有限公司、北京东方通科技股份有限公司、上海上讯信息技术股份有限公司、江苏君立华域信息安全技术股份有限公司、苏州棱镜七彩信息科技有限公司、博智安全科技股份有限公司、广东唯顶信息科技股份有限公司、广州安亿信软件科技有限公司、浙江木链物联网科技有限公司、湖北珞格科技发展有限公司、上海齐同信息科技有限公司、河北千诚电子科技有限公司、安徽长泰科技有限公司、上海纽盾科技股份有限公司、山东新潮信息技术有限公司、河南悦海数安科技有限公司、杭州迪普科技股份有限公司及其他个人白帽子向 CNVD 提交了 7225 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 5987 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） | 4282 | 4282 |
| 三六零数字安全科技集团有限公司 | 848 | 848 |
| 奇安信网神（补天平台） | 670 | 670 |
| 北京神州绿盟科技有限公司 | 589 | 3 |
| 深信服科技股份有限公司 | 299 | 0 |
| 新华三技术有限公司 | 286 | 0 |
| 北京数字观星科技有限公司 | 242 | 0 |
| 安天科技集团股份有限公司 | 225 | 2 |
| 南京众智维信息科技有限公司 | 201 | 201 |
| 上海交大 | 187 | 187 |
| 恒安嘉新（北京）科技股份公司 | 99 | 0 |
| 天津市国瑞数码安全系统股份有限公司 | 59 | 0 |
| 北京启明星辰信息安全技术有限公司 | 56 | 0 |

| | | |
|---|---|---|
| 杭州安恒信息技术股份有限公司 | 46 | 36 |
| 西安四叶草信息技术有限公司 | 35 | 35 |
| 中国电信集团系统集成有限责任公司 | 31 | 3 |
| 京东科技信息技术有限公司 | 29 | 0 |
| 北京知道创宇信息技术有限公司 | 18 | 1 |
| 北京长亭科技有限公司 | 11 | 11 |
| 南京联成科技发展股份有限公司 | 6 | 6 |
| 北京天融信网络安全技术有限公司 | 5 | 5 |
| 深圳市腾讯计算机系统有限公司（玄武实验室） | 4 | 4 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 2 | 2 |
| 沈阳东软系统集成工程有限公司 | 1 | 1 |
| 北京华顺信安信息技术有限公司 | 312 | 5 |
| 河南信安世纪科技有限公司 | 56 | 56 |
| 重庆都会信息科技有限公司 | 26 | 26 |
| 杭州迪普科技股份有限公司 | 22 | 1 |
| 河南东方云盾信息技术有限公司 | 20 | 20 |

| | | |
|---|---|---|
| 山石网科通信技术股份有限公司 | 12 | 12 |
| 北京山石网科信息技术有限公司 | 9 | 9 |
| 河南灵创电子科技有限公司 | 9 | 9 |
| 长春嘉诚信息技术股份有限公司 | 8 | 8 |
| 北京升鑫网络科技有限公司 | 5 | 5 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 4 | 4 |
| 中能融合智慧科技有限公司攻防实验室 | 4 | 4 |
| 江苏省信息安全测评中心 | 4 | 4 |
| 快页信息技术有限公司 | 3 | 3 |
| 联通沃悦读科技文化有限公司 | 3 | 3 |
| 北京君云天下科技有限公司 | 3 | 3 |
| 北京东方通科技股份有限公司 | 3 | 3 |
| 上海上讯信息技术股份有限公司 | 2 | 2 |
| 江苏君立华域信息安全技术股份有限公司 | 2 | 2 |
| 苏州棱镜七彩信息科技有限公司 | 2 | 2 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 广东唯顶信息科技股 | 1 | 1 |

| | | |
|---|---|---|
| 份有限公司 | | |
| 广州安亿信软件科技有限公司 | 1 | 1 |
| 浙江木链物联网科技有限公司 | 1 | 1 |
| 湖北珞格科技发展有限公司 | 1 | 1 |
| 上海齐同信息科技有限公司 | 1 | 1 |
| 河北千诚电子科技有限公司 | 1 | 1 |
| 安徽长泰科技有限公司 | 1 | 1 |
| 上海纽盾科技股份有限公司 | 1 | 1 |
| 山东新潮信息技术有限公司 | 1 | 1 |
| 河南悦海数安科技有限公司 | 1 | 1 |
| CNCERT 四川分中心 | 4 | 4 |
| CNCERT 内蒙古分中心 | 2 | 2 |
| CNCERT 山东分中心 | 1 | 1 |
| 个人 | 729 | 729 |
| 报送总计 | 9487 | 7225 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 320 个漏洞。WEB 应用 154 个，应用程序 79 个，网络设备（交换机、路由器等网络端设备）35 个，操作系统 23 个，安全产品 13 个，数据库 10 个，智能设备（物联网终端设备）6 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 | 154 |
| 应用程序 | 79 |
| 网络设备（交换机、路由器等网络端设备） | 35 |

| | |
|---|---|
| 操作系统 | 23 |
| 安全产品 | 13 |
| 数据库 | 10 |
| 智能设备（物联网终端设备） | 6 |

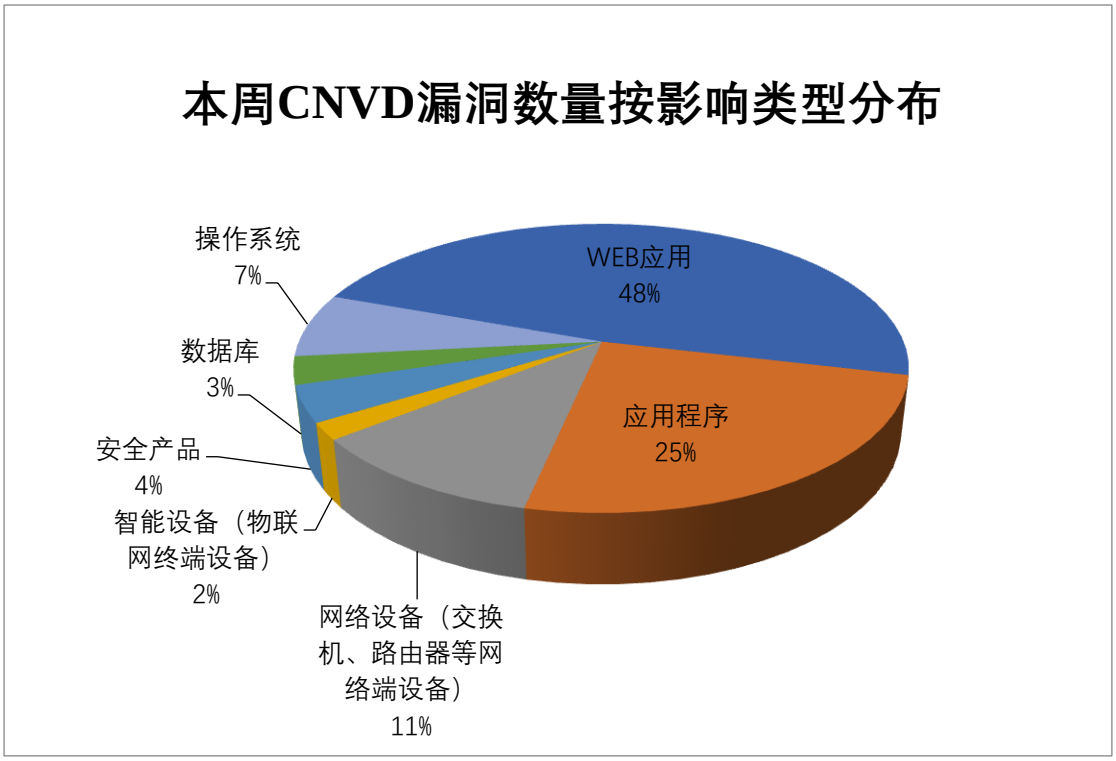


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Google、Apache 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 | 31 | 10% |
| 2 | Google | 18 | 6% |
| 3 | Apache | 14 | 4% |
| 4 | Microsoft | 13 | 4% |
| 5 | IBM | 12 | 4% |
| 6 | SWFTools | 10 | 3% |
| 7 | FFmpeg | 9 | 3% |
| 8 | 恒锋信息科技股份有限公司 | 7 | 2% |
| 9 | Huawei | 7 | 2% |
| 10 | 其他 | 199 | 62% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，25 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，“Google Android 权限提升漏洞（CNVD-2022-61751）、Siemens SCALANCE XM-400 和 XR-500 Devices 拒绝服务漏洞”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/

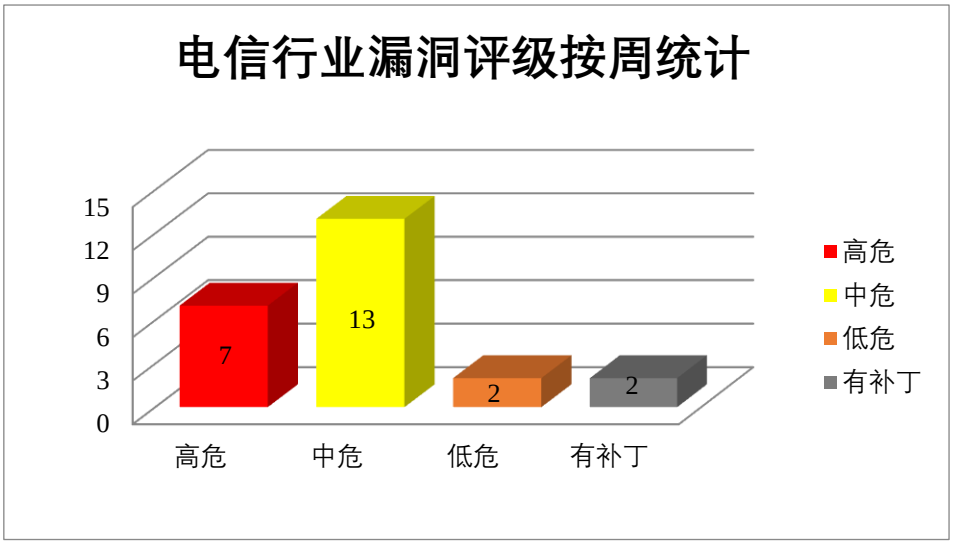


图 3 电信行业漏洞统计

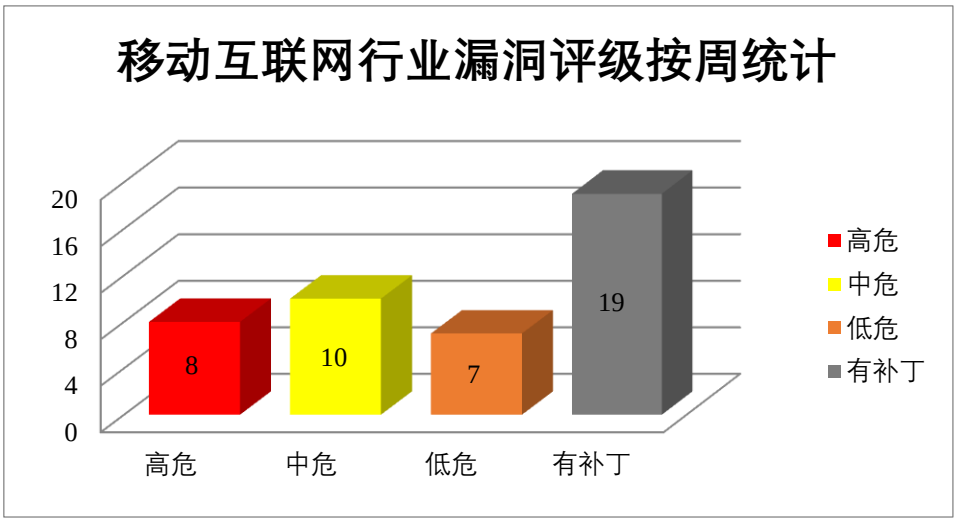


图 4 移动互联网行业漏洞统计

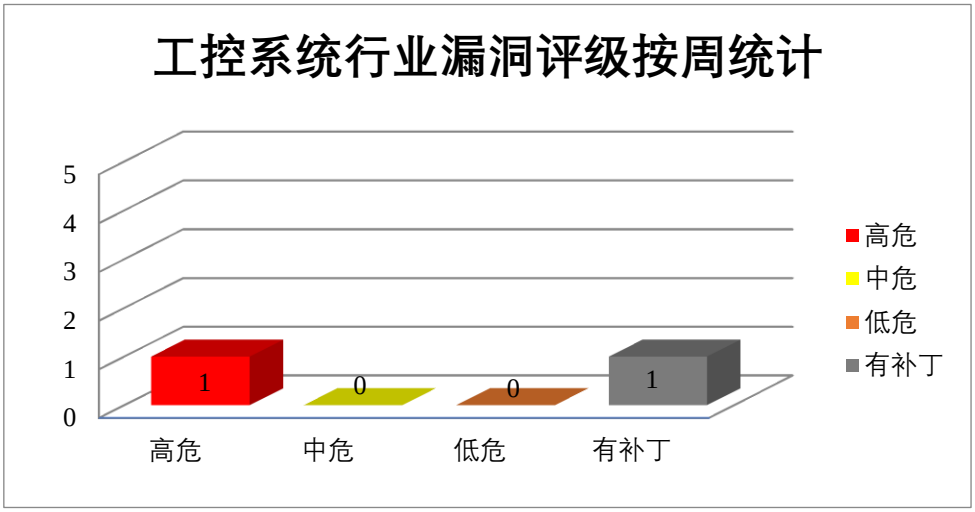


图 5 工控系统行业漏洞统计

## 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、Microsoft 产品安全漏洞

Microsoft Windows Print Spooler 是美国微软（Microsoft）公司的一个打印后台处理程序组件。Microsoft Windows Win32k 是美国微软（Microsoft）公司的一个用于 Windows 多用户管理的系统文件。Microsoft Windows Kerberos 是美国微软（Microsoft）公司的一个用于在网络集群中进行身份验证的软件。Kerberos 同时作为一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。Microsoft Hyper-V 是美国微软（Microsoft）公司的一个应用程序。一种系统管理程序虚拟化技术，能够实现桌面虚拟化。Microsoft Windows 是一款由美国微软公司开发的窗口化操作系统。Microsoft Windows Cluster Shared Volume 是美国微软（Microsoft）公司的一项功能。Microsoft Hyper-V 是美国微软（Microsoft）公司的一个应用程序。一种系统管理程序虚拟化技术，能够实现桌面虚拟化。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，在系统上执行任意代码，造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Microsoft Windows Print Spooler 权限提升漏洞（CNVD-2022-62513、CNVD-2022-62512）、Microsoft Windows Win32k 权限提升漏洞（CNVD-2022-62516）、Microsoft Windows Kerberos 权限提升漏洞、Microsoft Windows Hyper-V Shared Virtual Hard Disks 信息泄露漏洞（CNVD-2022-62514）、Microsoft Windows DNS Server 远程代码执行漏洞、Microsoft Windows Cluster Shared Volume (CSV) 拒绝服务漏洞、Microsoft Windows Hyper-V Shared Virtual Hard Disks 信息泄露漏洞。其中，“Microsoft Windows DNS Server 远程代码执行漏洞”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-2022-62513

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62512

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62516

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62515

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62514

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62519

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62518

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62517

### 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，攻击者可利用漏洞获取敏感信息，提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-61747、CNVD-2022-61746、CNVD-2022-61751、CNVD-2022-61754）、Google Android 信息泄露漏洞（CNVD-2022-61749、CNVD-2022-61753）、Google Android 越界写入漏洞（CNVD-2022-61752）、Google Android 远程代码执行漏洞（CNVD-2022-61757）。其中，“Google Android 权限提升漏洞（CNVD-2022-61747、CNVD-2022-61751）、Google Android 越界写入漏洞（CNVD-2022-61752）、Google Android 远程代码执行漏洞（CNVD-2022-61757）”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-2022-61747

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61746

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61751

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61749

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61754

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61753

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61752

https://www.cnvd.org.cn/flaw/show/CNVD-2022-61757

### 3、 IBM 产品安全漏洞

IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM Security Identity Manager（ISIM）是美国 IBM 公司的一套身份管理和治理解决方案。该方案可在整个用户生命周期内自动创建、修改、重新认证和终止用户特权，并支持基于策略的密码管理。IBM Sterling B2B Integrator 是

美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。IBM App Connect Enterprise 是美国 IBM 公司的一个操作系统。IBM App Connect Enterprise 将现有业界信任的 IBM Integration Bus 技术与 IBM App Connect Professional 以及新的云本机技术进行了组合，提供一个可满足现代数字企业全面集成需求的平台。IBM Engineering Requirements Quality Assistant 是美国 IBM 公司的一款基于 Watson AI 用于辅助开发人员提高工程需求质量的软件。该应用可显著降低发现缺陷成本，有利于尽早发现工程流程中的需求错误，加快产品上市。IBM Sterling File Gateway 是美国 IBM 公司的一套文件传输软件。该软件可整合不同的文件传输活动中心，并帮助基于文件的数据通过因特网实现安全交换。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，伪造用户身份，发送恶意请求，执行非法 SQL 命令窃取数据库敏感数据，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2022-61905）、IBM Security Identity Manager 开放重定向漏洞、IBM Sterling B2B Integrator 授权问题漏洞（CNVD-2022-61908）、IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2022-61907）、IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2022-61906）、IBM App Connect Enterprise 拒绝服务漏洞、IBM Engineering Requirements Quality Assistant 跨站请求伪造漏洞、IBM Sterling File Gateway 信息泄露漏洞（CNVD-2022-61909）。其中，“IBM Sterling B2B Integrator 授权问题漏洞（CNVD-2022-61908）、IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2022-61906）、IBM Engineering Requirements Quality Assistant 跨站请求伪造漏洞”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-2022-61905
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61904
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61908
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61907
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61906
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61911
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61910
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61909

### 4、 Apache 产品安全漏洞

Apache Avro 是美国阿帕奇（Apache）基金会的一个数据序列化系统。为 Apache Hadoop 提供数据序列化和数据交换服务。Apache JSPWiki 是美国阿帕奇（Apache）基金会的一款基于 Java、Servlet 和 JSP 构建的开源 WikiWiki 引擎。Apache Shiro 是一个

使用的 Java 安全框架，功能包括身份验证、授权、加密和会话管理。Apache Sling 是美国阿帕奇（Apache）基金会的一个 Java 平台的开源 Web 框架。旨在在符合 JSR-170 的内容存储库（例如 Apache Jackrabbit ）上创建以内容为中心的应用程序。Apache Hadoop 是美国阿帕奇（Apache）基金会的一套开源的分布式系统基础架构。Apache Apisix 是美国阿帕奇（Apache）基金会的一个云原生的微服务 API 网关服务。该软件基于 OpenResty 和 etcd 来实现，具备动态路由和插件热加载，适合微服务体系下的 API 管理。Apache Commons Compress 是美国阿帕奇（Apache）基金会的一个用于处理压缩文件的库。Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过网络限制，提升权限，导致程序崩溃等。

CNVD 收录的相关漏洞包括：Apache Avro 拒绝服务漏洞、Apache JSPWiki 跨站请求伪造漏洞（CNVD-2022-61913）、APACHE SHIRO 身份验证绕过漏洞、Apache Sling 日志注入漏洞、Apache Hadoop 参数注入漏洞、Apache APISIX 访问控制错误漏洞、Apache Commons Compress 资源管理错误漏洞（CNVD-2022-62077）、Apache Airflow 授权问题漏洞（CNVD-2022-62076）。其中，除“Apache Sling 日志注入漏洞、Apache APISIX 访问控制错误漏洞、Apache Commons Compress 资源管理错误漏洞（CNVD-2022-62077）”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-2022-61912
https://www.cnvd.org.cn/flaw/show/CNVD-2022-61913
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62075
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62074
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62073
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62078
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62077
https://www.cnvd.org.cn/flaw/show/CNVD-2022-62076

### 5、LibreHealth EHR 跨站脚本漏洞（CNVD-2022-62206）

LibreHealth EHR 是一个以临床为中心的电子健康记录 (EHR) 系统，其设计既易于开箱即用使用，也可定制用于各种医疗保健环境。本周，LibreHealth EHR 被披露存在跨站脚本漏洞。该漏洞源于 interface/main/finder/finder_navigation.php 页面对于参数缺少过滤和转义。攻击者可利用该漏洞在客户端执行 JavaScript 代码。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-2022-62206

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-2022-61751 | Google Android 权限提升漏洞（CNVD-2022-61751） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/pixel/2022-07-01 |
| CNVD-2022-61757 | Google Android 远程代码执行漏洞（CNVD-2022-61757） | 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-2022-61906 | IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2022-61906） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6612505 |
| CNVD-2022-61913 | Apache JSPWiki 跨站请求伪造漏洞（CNVD-2022-61913） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2022-34158 |
| CNVD-2022-62073 | Apache Hadoop 参数注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/mxqnb39jfrwgs3j6phwvlrfq4mlox130 |
| CNVD-2022-62219 | Vim 资源管理错误漏洞（CNVD-2022-62219） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim/ |
| CNVD-2022-62224 | BlueZ 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://ubuntu.com/security/notices/USN-5481-1 |
| CNVD-2022-62235 | SQLite 输入验证错误漏洞（CNVD-2022-62235） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.sqlite.org/cgi/docsrc/info/6c12812e54d369d5ba596fba91c29f08b325d237f69eace6e6eb6feed835c817 |
| CNVD-2022-62366 | PublicCMS 服务器端请求伪造漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/sanluan/PublicCMS/ |
| CNVD-2022-62519 | Microsoft Windows DNS Server 远程代码执行漏洞 | 高 | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： |

| | | | |
|---|---|---|---|
| | | | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24547 |

小结：本周，Microsoft 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，在系统上执行任意代码，造成拒绝服务情况等。此外，Google、IBM、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过网络限制，获取敏感信息，提升权限，在系统上执行任意代码，导致拒绝服务等。另外，LibreHealth EHR 被披露存在跨站脚本漏洞。攻击者可利用该漏洞在客户端执行 JavaScript 代码。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、 Contec SolarView Compact 远程代码执行漏洞

**验证描述**

Contec SolarView Compact 是日本 Contec 公司的一个应用系统。提供光伏发电测量系统。

Contec SolarView Compact v6.0 版本存在远程代码执行漏洞，该漏洞源于 Solar_Image.php 未能正确过滤构造代码段的特殊元素。攻击者可利用该漏洞执行任意代码。

**验证信息**

POC 链接：https://github.com/badboycxcc/SolarView_Compact_6.0_upload

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-61893

**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. Apache IoTDB grafana-connector 模块存在未授权漏洞

开源项目 Apache IoTDB grafana-connector 模块存在未授权漏洞，攻击者可以未授权问/query、/search 接口，进而通过 web 服务可能会获取数据库的内部结构。

参考链接：https://www.4hou.com/posts/l6L6

### 2. CI/CD 管道中的代码注入漏洞影响 Google、Apache 开源 GitHub 项目

CI/CD 管道中存在安全漏洞，攻击者可以利用这些漏洞来破坏开发过程并在部署时

推出恶意代码。

参考链接：https://www.freebuf.com/news/343842.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