# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2023 年 01 月 16 日-2023 年 01 月 29 日** **2023 年第3、4 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 531 个，其中高危漏洞 255 个、中危漏洞 242 个、低危漏洞 34 个。漏洞平均分值为 6.55。本周收录的漏洞中，涉及 0day 漏洞 410 个（占 77%），其中互联网上出现“TP-Link TL-WR841N 跨站脚本漏洞、Online Diagnostic Lab Management System SQL 注入漏洞（CNVD-2023-04335）”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 4853 个，与上周（4084 个）环比增加 19%。

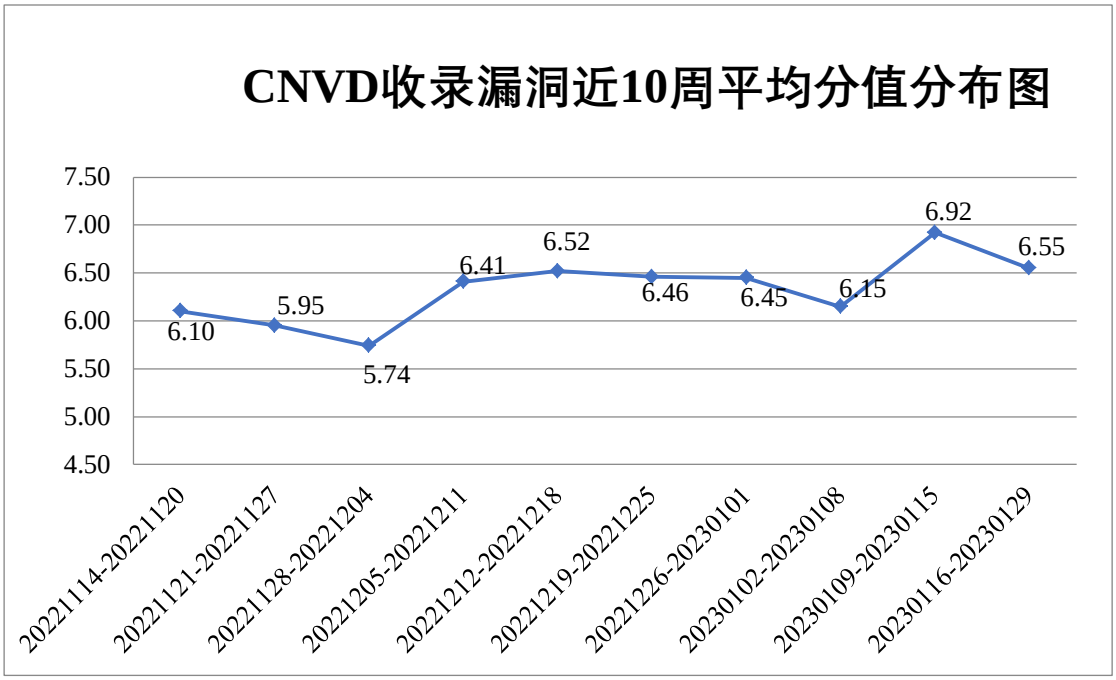


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 45 起，向基础电

信企业通报漏洞事件 50 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 1397 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 237 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 86 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：

淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、珠海国津软件科技有限公司、浙江浙大中控信息技术有限公司、浙江花田网络有限公司、长沙友点软件科技有限公司、昱能科技股份有限公司、用友网络科技股份有限公司、新天科技股份有限公司、新都（青岛）办公系统有限公司、武汉金同方科技有限公司、微软（中国）有限公司、网神信息技术（北京）股份有限公司、同望科技股份有限公司、苏州来呀电子商务有限公司、深圳市智博通电子有限公司、深圳市明源云科技有限公司、深圳市绿巨能科技发展有限公司、深圳市科荣软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳科士达科技股份有限公司、上海卓卓网络科技有限公司、上海逐一软件科技有限公司、上海煦声电子科技有限公司、上海宽惠网络科技股份有限公司、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、陕西融达信息科技有限公司、山西复盛公健康药业有限公司、山东山大电力技术股份有限公司、山东欧倍尔软件科技有限责任公司、厦门易达优送物流有限公司、若依、麒麟软件有限公司、南京未来物联科技有限公司、南京东大智能化系统有限公司、南大傲拓科技江苏股份有限公司、金蝶天燕云计算股份有限公司、华硕电脑（上海）有限公司、河北汉潮科技有限公司、杭州雄伟科技开发股份有限公司、杭州阔知网络科技有限公司、杭州海康威视数字技术股份有限公司、海南易而优科技有限公司、广州齐博网络科技有限公司、广西百益农业工程技术有限公司、东莞市珍艺苑文化传播有限公司、东方网力科技股份有限公司、大唐电信科技股份公司、冲电气实业(深圳)有限公司、北京云迹科技股份有限公司、北京用友政务软件股份有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京神指飞扬科技有限公司、北京龙软科技股份有限公司、北京光环新网科技股份有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、安徽中技国医医疗科技有限公司、阿里巴巴集团安全应急响应中心。

本周，CNVD 发布了《Oracle 发布 2023 年 1 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8501

## 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、新华三技术有限公司、西安四叶草信息技术有限公司、北京启明星辰信息安全技术有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。上海齐同信息科技有限公司、快页信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、内蒙古洞明科技有限公司、重庆都会信息科技有限公司、杭州默安科技有限公司、中国工商银行股份有限公司软件开发中心、赛尔网络有限公司、山东云天安全技术有限公司、重庆易阅科技有限公司、安徽锋刃信息科技有限公司、杭州美创科技有限公司、云南联创网安科技有限公司、广州安亿信软件科技有限公司、上海纽盾科技股份有限公司、北京墨云科技有限公司、平安银河实验室、博智安全科技股份有限公司、江苏国泰新点软件有限公司、博雅正链（北京）科技有限公司、武汉非尼克斯软件技术有限公司、南方电网数字电网集团信息通信科技有限公司、北京宇天恒瑞科技发展有限公司、河南灵创电子科技有限公司、郑州埃文科技、北京微步在线科技有限公司、山东新潮信息技术有限公司及其他个人白帽子向 CNVD 提交了 4853 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）、上海交大和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 3013 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 |
|---|---|---|
| 上海交大 | 1462 | 1462 |
| 奇安信网神（补天平台） | 890 | 890 |
| 斗象科技（漏洞盒子） | 661 | 661 |
| 北京神州绿盟科技有限公司 | 504 | 1 |
| 新华三技术有限公司 | 229 | 0 |
| 西安四叶草信息技术有限公司 | 175 | 175 |
| 北京启明星辰信息安全技术有限公司 | 126 | 0 |
| 阿里云计算有限公司 | 122 | 0 |
| 恒安嘉新（北京）科技股份公司 | 122 | 0 |
| 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 | 29 | 0 |

| | | |
|---|---|---|
| 北京长亭科技有限公司 | 11 | 11 |
| 北京数字观星科技有限公司 | 11 | 0 |
| 京东科技信息技术有限公司 | 8 | 8 |
| 南京众智维信息科技有限公司 | 3 | 3 |
| 北京智游网安科技有限公司 | 2 | 2 |
| 深圳市腾讯计算机系统有限公司（玄武实验室） | 1 | 1 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 1 | 1 |
| 北京知道创宇信息技术有限公司 | 1 | 0 |
| 上海齐同信息科技有限公司 | 116 | 116 |
| 快页信息技术有限公司 | 64 | 64 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 52 | 52 |
| 河南东方云盾信息技术有限公司 | 38 | 38 |
| 内蒙古洞明科技有限公司 | 22 | 22 |
| 重庆都会信息科技有限公司 | 20 | 20 |
| 杭州默安科技有限公司 | 17 | 17 |
| 中国工商银行股份有限公司软件开发中心 | 14 | 14 |

| | | |
|---|---|---|
| 赛尔网络有限公司 | 8 | 8 |
| 山东云天安全技术有限公司 | 7 | 7 |
| 重庆易阅科技有限公司 | 5 | 5 |
| 安徽锋刃信息科技有限公司 | 4 | 4 |
| 杭州美创科技有限公司 | 4 | 4 |
| 云南联创网安科技有限公司 | 3 | 3 |
| 北京华顺信安信息技术有限公司 | 2 | 0 |
| 广州安亿信软件科技有限公司 | 2 | 2 |
| 上海纽盾科技股份有限公司 | 2 | 2 |
| 北京墨云科技有限公司 | 2 | 2 |
| 平安银河实验室 | 2 | 2 |
| 亚信科技（成都）有限公司 | 1 | 0 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 江苏国泰新点软件有限公司 | 1 | 1 |
| 博雅正链（北京）科技有限公司 | 1 | 1 |
| 武汉非尼克斯软件技术有限公司 | 1 | 1 |
| 南方电网数字电网集团信息通信科技有限公司 | 1 | 1 |
| 北京宇天恒瑞科技发展有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 河南灵创电子科技有限公司 | 1 | 1 |
| 郑州埃文科技 | 1 | 1 |
| 北京微步在线科技有限公司 | 1 | 1 |
| 山东新潮信息技术有限公司 | 1 | 1 |
| CNCERT 甘肃分中心 | 8 | 8 |
| CNCERT 宁夏分中心 | 1 | 1 |
| CNCERT 贵州分中心 | 1 | 1 |
| 个人 | 1236 | 1236 |
| 报送总计 | 6029 | 4853 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 531 个漏洞。WEB 应用 331 个，应用程序 99 个，网络设备（交换机、路由器等网络端设备）56 个，智能设备（物联网终端设备）23 个，安全产品 13 个，操作系统 7 个，数据库 2 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 | 331 |
| 应用程序 | 99 |
| 网络设备（交换机、路由器等网络端设备） | 56 |
| 智能设备（物联网终端设备） | 23 |
| 安全产品 | 13 |
| 操作系统 | 7 |
| 数据库 | 2 |

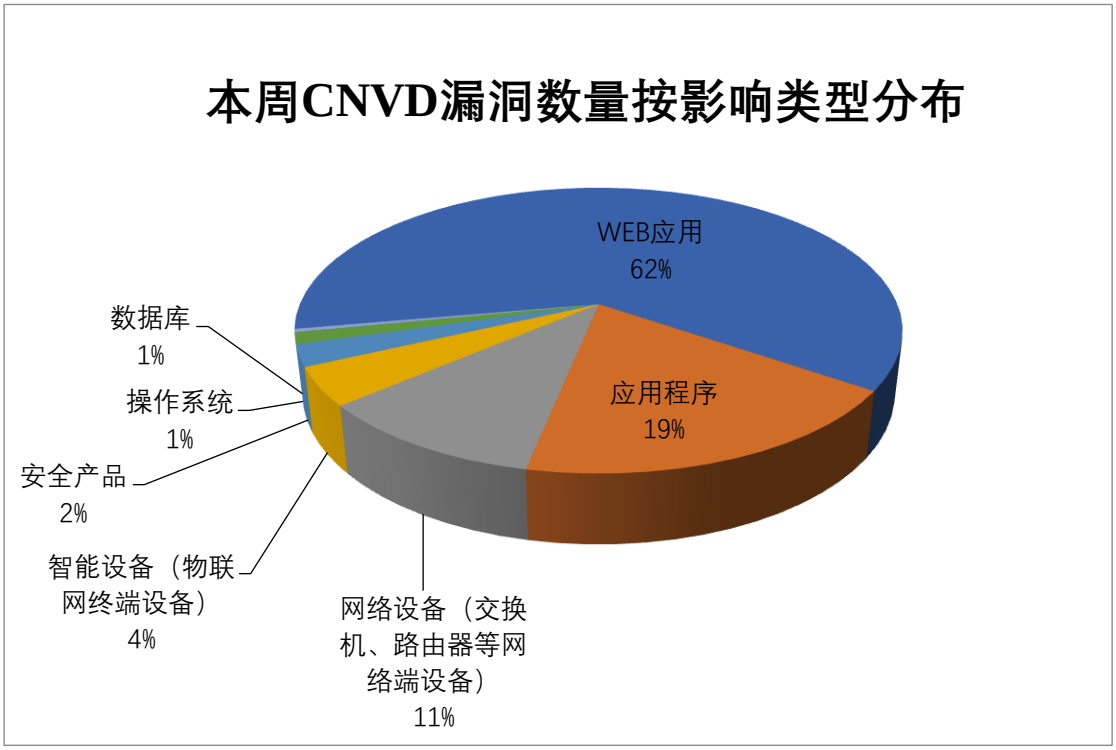


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apache、WordPress、Mozilla 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 | Apache | 22 | 4% |
| 2 | WordPress | 22 | 4% |
| 3 | Mozilla | 15 | 3% |
| 4 | Microsoft | 15 | 2% |
| 5 | Google | 12 | 2% |
| 6 | 商派软件有限公司 | 10 | 2% |
| 7 | 北京百卓网络技术有限公司 | 10 | 2% |
| 8 | 用友网络科技股份有限公司 | 9 | 2% |
| 9 | College Management System | 9 | 2% |
| 10 | 其他 | 407 | 77% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 37 个电信行业漏洞，33 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，“Oracle WebLogic Server 远程代码执行漏洞（CNVD-

2023-04389）”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/

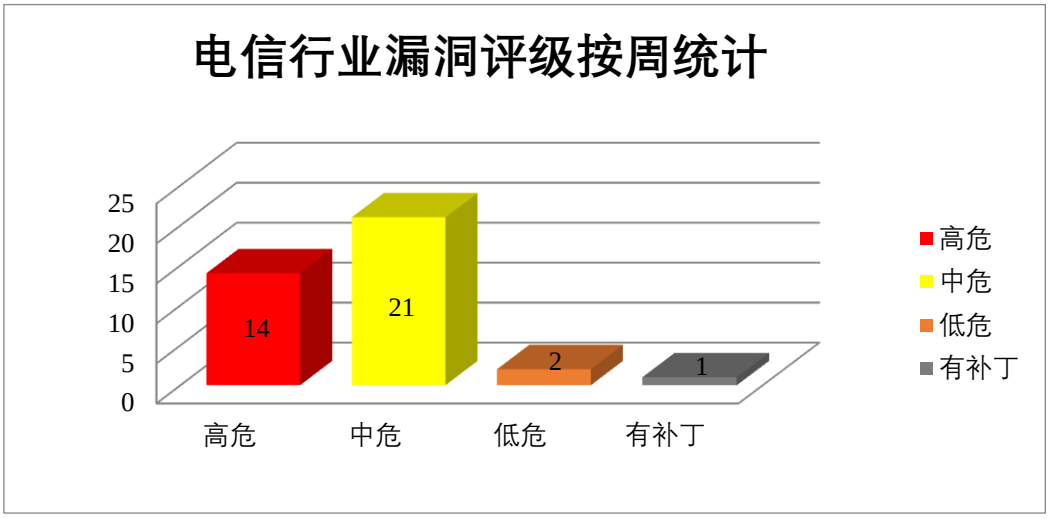


图 3 电信行业漏洞统计

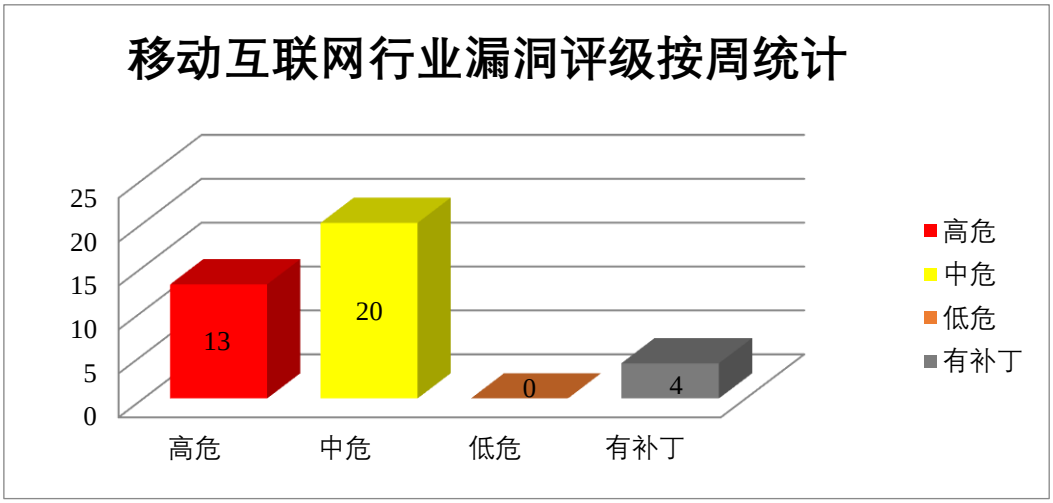


图 4 移动互联网行业漏洞统计

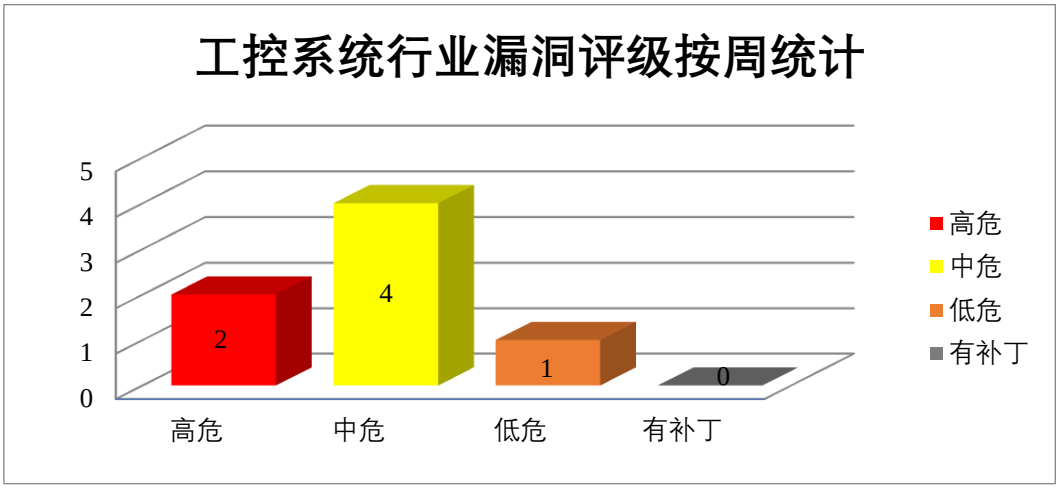


图 5 工控系统行业漏洞统计

## 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、 Apache 产品安全漏洞

Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache Traffic Server（ATS）是一套可扩展的 HTTP 代理和缓存服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞请求安全资源，执行任意代码等。

CNVD 收录的相关漏洞包括：Apache OFBiz 代码注入漏洞（CNVD-2023-03919、CNVD-2023-03918）、Apache OFBiz 代码问题漏洞（CNVD-2023-03920）、Apache Traffic Server 输入验证错误漏洞（CNVD-2023-03923、CNVD-2023-03927、CNVD-2023-03926、CNVD-2023-03925、CNVD-2023-03924）。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-2023-03919

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03918

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03920

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03923

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03927

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03926

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03925

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03924

### 2、 Google 产品安全漏洞

Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源

平台。Google Chrome 是一款 Web 浏览器。Google Android 是一套以 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，攻击者可利用漏洞绕过安全限制，提升权限，在系统上执行任意代码，导致越界内存读取或崩溃等。

CNVD 收录的相关漏洞包括：Google TensorFlow 缓冲区溢出漏洞（CNVD-2023-03935、CNVD-2023-03936）、Google Chrome 安全绕过漏洞（CNVD-2023-04547）、Google Android 权限提升漏洞（CNVD-2023-04551、CNVD-2023-04552、CNVD-2023-04553）、Google Chrome Forms 代码执行漏洞、Google Chrome Extensions 代码执行漏洞（CNVD-2023-04555）。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-2023-03935
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03936
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04547
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04551
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04552
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04553
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04554
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04555

### 3、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使脚本在无效对象状态下执行导致绕过安全限制，执行任意代码，造成浏览器崩溃等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-03061、CNVD-2023-03062、CNVD-2023-03064、CNVD-2023-03066）、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-03067、CNVD-2023-03063）、Mozilla Firefox 代码问题漏洞（CNVD-2023-03065）、Mozilla Firefox 访问控制错误漏洞（CNVD-2023-03068）。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-2023-03061
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03062
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03065
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03064
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03063
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03066
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03068

https://www.cnvd.org.cn/flaw/show/CNVD-2023-03067

### 4、SAP 产品安全漏洞

SAP Host Agent 是德国思爱普（SAP）公司的一套支持操作系统监视、数据库监视和系统实例监视等多项生命周期管理任务的代理程序。SAP BusinessObjects Business Intelligence Platform 是一款完备的商务分析平台。该平台集市场领先的 SAP 数据整合产品、数据管理产品和商务智能 (BI) 产品于一身，可消除系统集成难题，快速、轻松地部署高性能的商务分析软件。SAP NetWeaver AS 是一款 SAP 网络应用服务器。它不仅能提供网络服务，且还是 SAP 软件的基本平台。SAP Bank Account Management 是一个银行账户管理系统。SAP BPC MS 是一个业务规划与整合应用程序。提供规划、预算、预测和财务合并功能。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，执行非法 SQL 命令窃取数据库敏感数据，导致跨站脚本攻击，任意代码执行等。

CNVD 收录的相关漏洞包括：SAP Host Agent 访问控制错误漏洞、SAP Business Objects Business Intelligence Platform 跨站脚本漏洞（CNVD-2023-03049）、SAP BusinessObjects Business Intelligence Platform CMC application 跨站脚本漏洞、SAP NetWeaver AS 访问控制错误漏洞、SAP Bank Account Management 信息泄露漏洞、SAP BusinessObjects Analysis(Edition For Olap)代码注入漏洞、SAP BPC MS SQL 注入漏洞、SAP NetWeaver Application Server 跨站脚本漏洞（CNVD-2023-04301）。其中，“SAP BusinessObjects Business Intelligence Platform CMC application 跨站脚本漏洞、SAP NetWeaver AS 访问控制错误漏洞、SAP BusinessObjects Analysis(Edition For Olap)代码注入漏洞、SAP BPC MS SQL 注入漏洞”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-2023-03050
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03049
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03048
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03052
https://www.cnvd.org.cn/flaw/show/CNVD-2023-03051
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04300
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04302
https://www.cnvd.org.cn/flaw/show/CNVD-2023-04301

### 5、WordPress plugin LetsRecover SQL 注入漏洞

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。WordPress 是一套使用 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 是一个应用插件。本周，WordPress plugin LetsRecover 被披露

存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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-2023-04535

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-2023-03046 | Linux kernel ksmbd 模块缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/torvalds/linux/commit/797805d81baa814f76cf7bdab35f86408a79d 707 |
| CNVD-2023-03054 | Mozilla Thunderbird 资源管理错误漏洞（CNVD-2023-03054） | 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.mozilla.org/en-US/security/advisories/mfsa2022-53/ |
| CNVD-2023-03055 | Mozilla Firefox 注入漏洞（CNVD-2023-03055） | 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.mozilla.org/en-US/security/advisories/mfsa2022-51/ |
| CNVD-2023-03932 | Siemens syngo Dynamics 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://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 |
| CNVD-2023-04306 | Adobe InDesign 缓冲区溢出漏洞（CNVD-2023-04306） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/indesign/apsb23-07.html |
| CNVD-2023-04310 | Publify 输入验证错误漏洞（CNVD-2023-04310） | 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/publify/publify/commit/ca46da283572b4f8c0b5aa245008756c8a5fd1b1 |
| CNVD-2023-04307 | Adobe InDesign 输入验证错误漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/indesign/apsb23-07.html |
| CNVD-2023-04313 | phpMyFAQ 跨站脚本漏洞（CNVD-2023-04313） | 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/thorsten/phpMyFA |

| | | | |
|---|---|---|---|
| | | | Q/releases/tag/3.1.10 |
| CNVD-2023-04319 | Microsoft 3D Builder 远程代码执行漏洞（CNVD-2023-04319） | 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/en-US/security-guidance/advisory/CVE-2023-21792 |
| CNVD-2023-04322 | Microsoft 3D Builder 远程代码执行漏洞（CNVD-2023-04322） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21788 |

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用漏洞请求安全资源，执行任意代码等。此外，Google、Mozilla、SAP 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，绕过安全限制，提升权限，在系统上执行任意代码，导致越界内存读取，跨站脚本攻击或崩溃等。另外，WordPress plugin LetsRecover 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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、Online Diagnostic Lab Management System SQL 注入漏洞（CNVD-2023-04335）**

**验证描述**

Online Diagnostic Lab Management System 是在线诊断实验室管理系统。

Online Diagnostic Lab Management System v1.0 版本存在 SQL 注入漏洞，该漏洞源于缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞获取数据库敏感信息。

**验证信息**

POC 链接：https://github.com/vickysuper/Cve_report/blob/master/vendors/oretnom23/online-diagnostic-lab-management-system/SQLi-3.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-04335

**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. WAN 路由器 IP 更改导致 Microsoft 365 大规模中断

微软表示，长达 5 小时的微软 365 全球停机是由路由器 IP 地址更改导致的，该更改导致了其广域网中所有其他路由器之间的数据包转发问题。

参考链接：https://www.bleepingcomputer.com/news/microsoft/massive-microsoft-365-outage-caused-by-wan-router-ip-change/

### 2. Zoho ManageEngine OnPremise 多款产品远程代码执行漏洞安全风险通告

Zoho ManageEngine OnPremise 多款产品如 ADManager Plus 中存在远程代码执行漏洞，在当前已启用或曾经启用过 SAML 单点登录的状态下，未经授权的远程攻击者可利用此漏洞在目标服务器上执行任意代码。

参考链接：https://www.secrss.com/articles/51375

### 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