# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2024 年 01 月 29 日-2024 年 02 月 04 日** **2024 年第 5 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 409 个，其中高危漏洞 177 个、中危漏洞 225 个、低危漏洞 7 个。漏洞平均分值为 6.60。本周收录的漏洞中，涉及 0day 漏洞 283 个（占 69%），其中互联网上出现“SEMCMS SQL 注入漏洞（CNVD-2024-06232）、Gila CMS Area 参数 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 13040 个，与上周（12980 个）环比增加 0.5%。

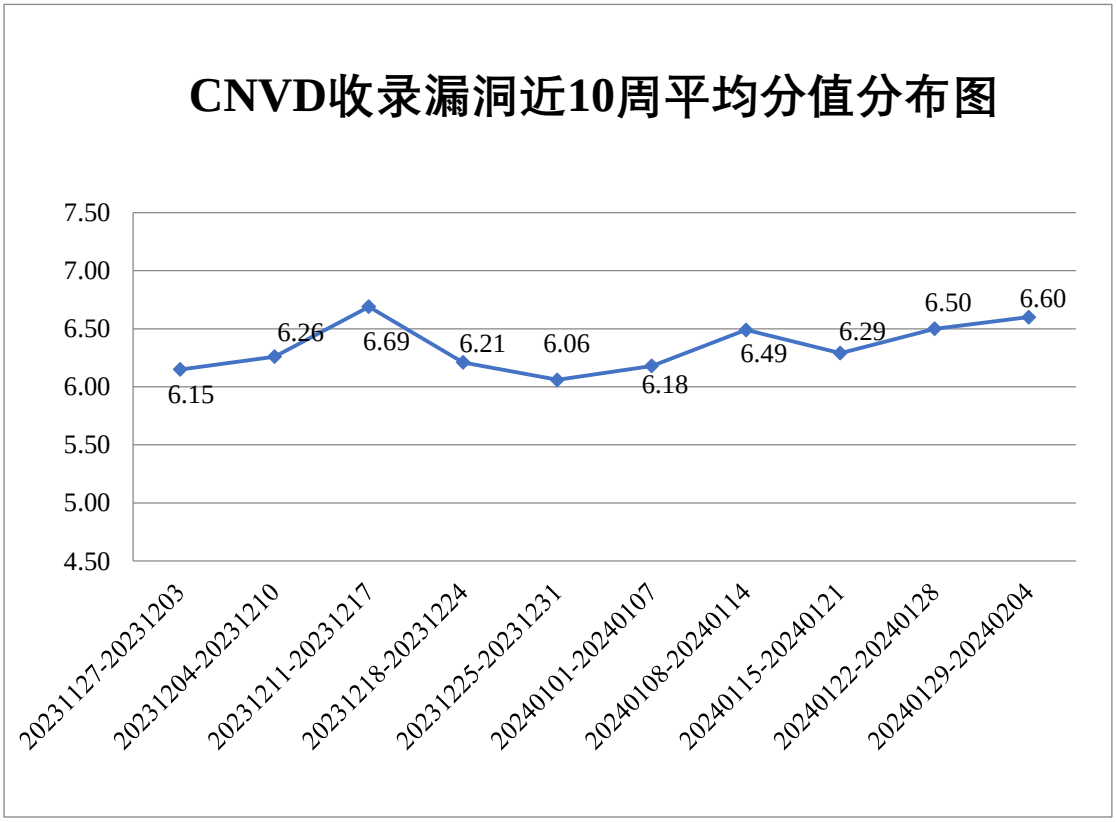


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 27 起，向基础电信企业通报漏洞事件 15 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 744 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 75 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 65 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：

珠海世纪鼎利科技股份有限公司、珠海金山办公软件有限公司、中金易云科技有限责任公司、中国软件与技术服务股份有限公司、智互联（深圳）科技有限公司、浙江华途信息安全技术股份有限公司、浙江和达科技股份有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永服科技有限公司、英万齐软件技术（北京）有限公司、音数汇元（上海）智能科技有限公司、新疆生产建设兵团住房和城乡建设局、西安西瑞控制技术股份有限公司、西安图安云算信息科技有限公司、西安旌旗电子股份有限公司、武汉金同方科技有限公司、武汉达梦数据库有限公司、武汉北科天翼科技有限公司、天津天堰科技股份有限公司、泰安梦泰尔软件有限公司、台安科技（无锡）有限公司、苏州汉明科技有限公司、四平市九州易通科技有限公司、四川易泊时捷智能科技有限公司、四川迅睿云软件开发有限公司、世邦通信股份有限公司、深圳中台威堡科技有限公司、深圳希施玛数据科技有限公司、深圳市中电电力技术股份有限公司、深圳市美科星通信技术有限公司、深圳市蓝凌软件股份有限公司、深圳市嘉荣华科技有限公司、深圳市昂捷信息技术股份有限公司、深圳市安之源电子有限公司、深圳金三立视频科技股份有限公司、深圳古瑞瓦特新能源有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海小羚羊软件有限公司、上海司南卫星导航技术股份有限公司、上海商鼎软件科技有限公司、上海寰创通信科技股份有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、上海艾泰科技有限公司、山东比特智能科技股份有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、三未信安科技股份有限公司、青岛海信网络科技股份有限公司、普联技术有限公司、品茗科技股份有限公司、鹏为软件股份有限公司、内蒙古华腾科技股份有限公司、南京安元科技有限公司、蓝网科技股份有限公司、科大讯飞股份有限公司、金蝶软件（中国）有限公司、江苏群杰物联科技有限公司、江苏国泰新点软件有限公司、江华瑶族自治县觅道网络科技工作室、惠普贸易（上海）有限公司、湖北京山轻工机械股份有限公司、宏脉信息技术（广州）股份有限公司、杭州叙简科技股份有限公司、杭州海康威视数字技术股份有限公司、广州中望龙腾软件股份有限公司、广州市蓝海创新科技有限公司、广州南方测绘科技股份有限公司、广州华壹智能科技有限公司、广州和晖科技有限公司、广东天波信息技术股份有限公司、广东飞企互联科技股

份有限公司、富士胶片商业创新（中国）有限公司、福州创杰信息科技有限公司、福建科立讯通信有限公司、孚链艺术品鉴定认证有限公司、泛微网络科技股份有限公司、成都索贝数码科技股份有限公司、成都生动网络科技有限公司、成都德芯数字科技股份有限公司、北京中成科信科技发展有限公司、北京致远互联软件股份有限公司、北京易普行科技有限公司、北京亿赛通科技发展有限责任公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京通元动力软件技术有限责任公司、北京通达信科科技有限公司、北京润乾信息系统技术有限公司、北京龙软科技股份有限公司、北京朗新天霁软件技术有限公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京和欣运达科技有限公司、北京辰信领创信息技术有限公司、百家云集团有限公司、奥琦玮信息科技（北京）有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司和 Trend Micro。

## 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、北京天融信网络安全技术有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、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。江苏金盾检测技术股份有限公司、河南东方云盾信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、北京卓识网安技术股份有限公司、贵州多彩网安科技有限公司、安徽天行网安信息安全技术有限公司、快页信息技术有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、联想集团、深圳昂楷科技有限公司、含光实验室、安徽锋刃信息科技有限公司、杭州默安科技有限公司、湖南泛联新安信息科技有限公司、北京中关村实验室、任子行网络技术股份有限公司、上海观安信息技术股份有限公司、新疆海狼科技有限公司、海南神州希望网络有限公司、安全邦（北京）信息技术有限公司、北方实验室（沈阳）股份有限公司、贵州华黔信安信息技术有限公司、北京山石网科信息技术有限公司、浙江木链物联网科技有限公司、中孚安全技术有限公司、杭州寻臻科技有限责任公司、赛尔网络有限公司、中国电信股份有限公司上海研究院、北京墨云科技有限公司、博智安全科技股份有限公司、北京天防安全科技有限公司、河南悦海数安科技有限公司及其他个人白帽子向 CNVD 提交了 13040 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）、奇安信网神（补天平台）、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 11568 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） | 8837 | 8837 |
| 奇安信网神（补天平 | 1503 | 1503 |

| | | |
|---|---|---|
| 台） | | |
| 三六零数字安全科技集团有限公司 | 967 | 967 |
| 新华三技术有限公司 | 609 | 0 |
| 北京天融信网络安全技术有限公司 | 463 | 1 |
| 深信服科技股份有限公司 | 374 | 0 |
| 上海交大 | 261 | 261 |
| 北京神州绿盟科技有限公司 | 245 | 2 |
| 阿里云计算有限公司 | 210 | 1 |
| 北京启明星辰信息安全技术有限公司 | 165 | 9 |
| 安天科技集团股份有限公司 | 120 | 0 |
| 北京长亭科技有限公司 | 118 | 6 |
| 北京知道创宇信息技术有限公司 | 65 | 0 |
| 恒安嘉新（北京）科技股份公司 | 56 | 0 |
| 杭州安恒信息技术股份有限公司 | 43 | 17 |
| 杭州迪普科技股份有限公司 | 18 | 0 |
| 北京安信天行科技有限公司 | 18 | 18 |
| 中国电信股份有限公司网络安全产品运营中心 | 9 | 9 |
| 厦门服云信息科技有限公司 | 2 | 2 |
| 北京智游网安科技有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 江苏金盾检测技术股份有限公司 | 172 | 172 |
| 河南东方云盾信息技术有限公司 | 28 | 28 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 25 | 25 |
| 北京卓识网安技术股份有限公司 | 23 | 23 |
| 贵州多彩网安科技有限公司 | 21 | 21 |
| 安徽天行网安信息安全技术有限公司 | 18 | 18 |
| 快页信息技术有限公司 | 14 | 14 |
| 河南灵创电子科技有限公司 | 13 | 13 |
| 内蒙古洞明科技有限公司 | 11 | 11 |
| 联想集团 | 6 | 6 |
| 深圳昂楷科技有限公司 | 6 | 6 |
| 含光实验室 | 6 | 6 |
| 安徽锋刃信息科技有限公司 | 6 | 6 |
| 杭州默安科技有限公司 | 4 | 4 |
| 湖南泛联新安信息科技有限公司 | 4 | 4 |
| 北京中关村实验室 | 4 | 4 |
| 任子行网络技术股份有限公司 | 3 | 3 |
| 上海观安信息技术股份有限公司 | 3 | 3 |
| 新疆海狼科技有限公 | 3 | 3 |

| | | |
|---|---|---|
| 司 | | |
| 海南神州希望网络有限公司 | 3 | 3 |
| 安全邦（北京）信息技术有限公司 | 2 | 2 |
| 北方实验室（沈阳）股份有限公司 | 2 | 2 |
| 贵州华黔信安信息技术有限公司 | 2 | 2 |
| 北京山石网科信息技术有限公司 | 2 | 2 |
| 浙江木链物联网科技有限公司 | 1 | 1 |
| 中孚安全技术有限公司 | 1 | 1 |
| 杭州寻臻科技有限责任公司 | 1 | 1 |
| 赛尔网络有限公司 | 1 | 1 |
| 中国电信股份有限公司上海研究院 | 1 | 1 |
| 北京墨云科技有限公司 | 1 | 1 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 北京天防安全科技有限公司 | 1 | 1 |
| 河南悦海数安科技有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 4 | 4 |
| CNCERT 河北分中心 | 1 | 1 |
| 个人 | 1011 | 1011 |
| 报送总计 | 15490 | 13040 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 409 个漏洞。WEB 应用 181 个，网络设备（交换机、路由器等网络端设备）82 个，应用程序 71 个，操作系统 31 个，智能设备（物联网终端设备）23 个，安全产品 13 个，数据库 8 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 |
| 网络设备（交换机、路由器等网络端设备） | 82 |
| 应用程序 | 71 |
| 操作系统 | 31 |
| 智能设备（物联网终端设备） | 23 |
| 安全产品 | 13 |
| 数据库 | 8 |

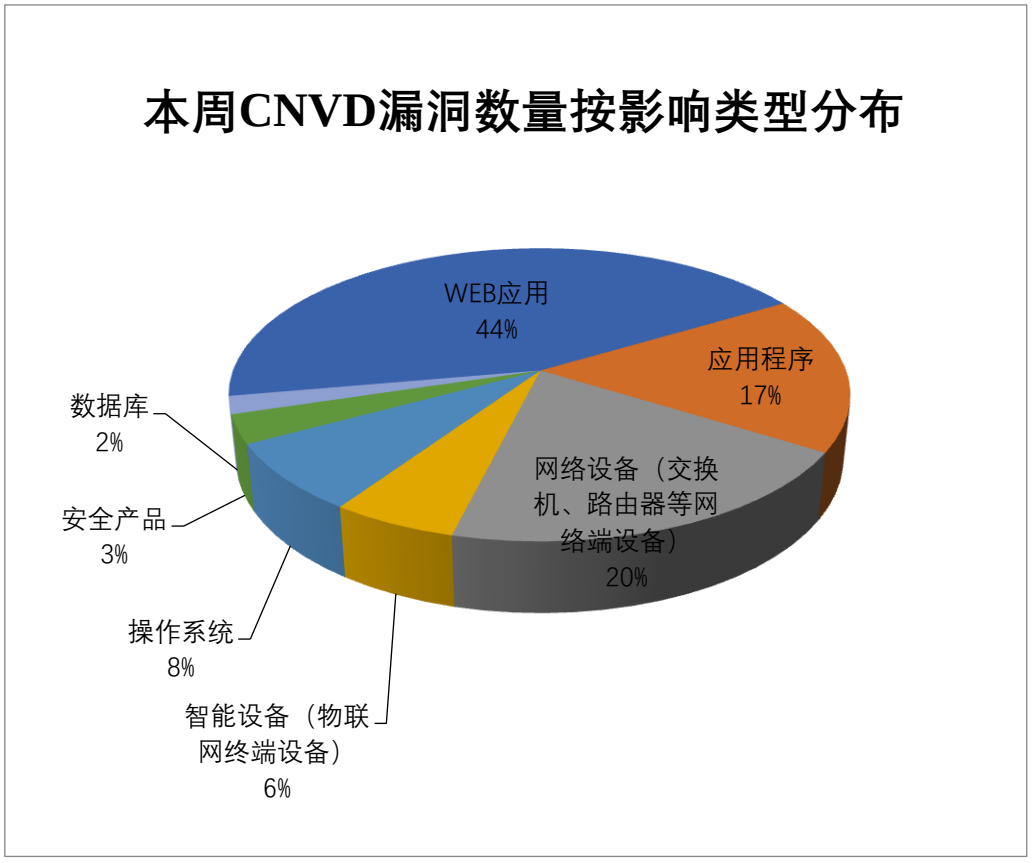


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、Google、Adobe 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 | 24 | 6% |
| 2 | Google | 21 | 5% |

| | | | |
|---|---|---|---|
| 3 | Adobe | 18 | 4% |
| 4 | 北京星网锐捷网络技术有限公司 | 14 | 3% |
| 5 | Apache | 12 | 3% |
| 6 | TOTOLINK | 11 | 3% |
| 7 | Fortinet | 10 | 3% |
| 8 | 用友网络科技股份有限公司 | 9 | 2% |
| 9 | 北京亿赛通科技发展有限责任公司 | 8 | 2% |
| 10 | 其他 | 282 | 69% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 68 个电信行业漏洞，36 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，“TOTOLINK X2000R 命令注入漏洞、D-Link DIR-815 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/

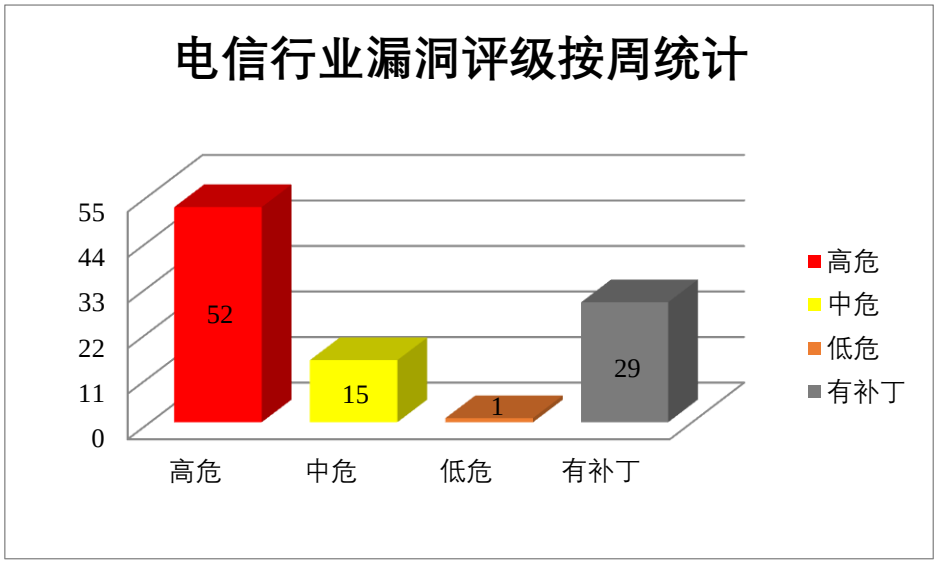


图 3 电信行业漏洞统计

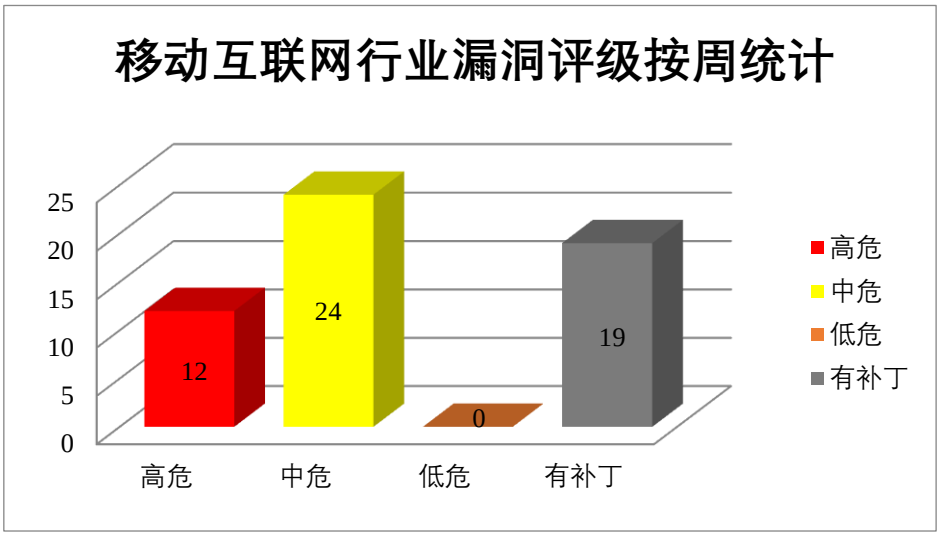


图 4 移动互联网行业漏洞统计

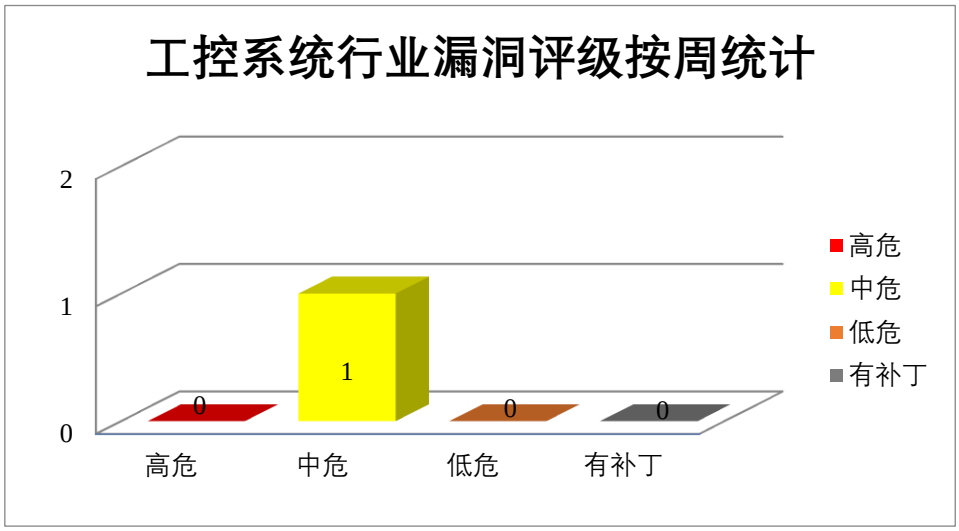


图 5 工控系统行业漏洞统计

## 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、 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，攻击者可利用漏洞在系统上执行任意代码，获得提升的权限。

CNVD 收录的相关漏洞包括：Google Android 代码执行漏洞（CNVD-2024-07123）、Google Android 权限提升漏洞（CNVD-2024-07112、CNVD-2024-07114、CNVD-2024-07115、CNVD-2024-07118、CNVD-2024-07125、CNVD-2024-07126、CNVD-2024-07127）。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-2024-07112
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07114
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07115
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07118
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07123
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07125
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07126
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07127

### 2、 Apache 产品安全漏洞

Apache InLong 是美国阿帕奇（Apache）基金会的一站式的海量数据集成框架。提供自动化、安全、可靠的数据传输能力。Apache StreamPark 是美国阿帕奇（Apache）基金会的一个流媒体应用程序开发框架。Apache Superset 是美国阿帕奇（Apache）基金会的一个数据可视化和数据探索平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注册 SQLite 数据库连接，使用导入图表功能错误地创建资源，插入命令进行远程命令执行等。

CNVD 收录的相关漏洞包括：Apache InLong 代码注入漏洞、Apache StreamPark 命令注入漏洞、Apache Superset 跨站脚本漏洞（CNVD-2024-06442）、Apache Superset 拒绝服务漏洞（CNVD-2024-06816、CNVD-2024-06814）、Apache Superset 安全绕过漏洞（CNVD-2024-06820、CNVD-2024-06819、CNVD-2024-06818）。其中，“Apache InLong 代码注入漏洞、Apache StreamPark 命令注入漏洞、Apache Superset 跨站脚本漏洞（CNVD-2024-06442）”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-2024-06239
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06256
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06442
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06816
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06814
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06820
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06819
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06818

### 3、 Fortinet 产品安全漏洞

Fortinet FortiPortal 是美国飞塔（Fortinet）公司的 FortiGate、FortiWiFi 和 FortiAP 产品线的高级、功能丰富的托管安全分析和管理支持工具，可作为虚拟机供 MSP 使用。Fortinet FortiPAM 是美国飞塔（Fortinet）公司的一款权限访问控制的平台。Fortinet Fo

rtiWeb 是美国飞塔（Fortinet）公司的一款 Web 应用层防火墙，它能够阻断如跨站点脚本、SQL 注入、Cookie 中毒、schema 中毒等攻击的威胁，保证 Web 应用程序的安全性并保护敏感的数据库内容。Fortinet FortiWLM 是美国飞塔（Fortinet）公司的一个无线管理器。Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web 内容过滤和反垃圾邮件等多种安全功能。Fortinet FortiMail 是美国飞塔（Fortinet）公司的一套电子邮件安全网关产品。该产品提供电子邮件安全防护和数据保护等功能。Fortinet FortiSIEM 是美国飞塔（Fortinet）公司的一套安全信息和事件管理系统。该系统包括资产发现、工作流程自动化和统一管理等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过精心设计的 Web 应用程序 URL 伪造流量日志，通过高频发送特制的 HTTP 或 HTTPS 请求来执行拒绝服务攻击，通过特制的请求执行未经授权的代码或命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiPortal 访问控制错误漏洞、Fortinet FortiPAM 资源管理错误漏洞、Fortinet FortiWeb 日志注入漏洞、Fortinet FortiWLM 操作系统命令注入漏洞、Fortinet FortiOS,FortiPAM 资源管理错误漏洞、Fortinet FortiMail 授权问题漏洞（CNVD-2024-06283、CNVD-2024-06288）、Fortinet FortiSIEM 命令执行漏洞（CNVD-2024-06289）。其中，除“Fortinet FortiPAM 资源管理错误漏洞、Fortinet FortiWeb 日志注入漏洞、Fortinet FortiMail 授权问题漏洞（CNVD-2024-06283）”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-2024-06230
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06229
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06253
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06255
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06254
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06283
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06289
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06288

### 4、Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-06261、CNVD-2024-06260、CNVD-2024-06259、CNVD-2024-06265、CNVD-2024-

06264、CNVD-2024-06263、CNVD-2024-06262、CNVD-2024-06268）。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-2024-06261
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06260
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06259
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06265
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06264
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06263
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06262
https://www.cnvd.org.cn/flaw/show/CNVD-2024-06268

**5、Tenda AX1803 缓冲区溢出漏洞**

Tenda AX1803 是中国腾达（Tenda）公司的一款双频千兆 WIFI6 路由器。本周，Tenda AX1803 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过组件/goform/SetOnlineDevName 运行任意代码。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-2024-06282

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

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-2024-06217 | IBM Security Access Manager Appliance 访问控制错误漏洞（CNVD-2024-06217） | 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/7106586 |
| CNVD-2024-06222 | TOTOLINK A3300R setTr069Cfg 方法命令注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html |
| CNVD-2024-06221 | TOTOLINK A3300R setScheduleCfg 方法命令注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html |
| CNVD-2024-06220 | TOTOLINK A3300R setNtpCfg 方法命令注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/ |

| | | | |
|---|---|---|---|
| | | | detail/menu_listtpl/download/id/241/ids/36.html |
| CNVD-2024-06233 | Tenda AX1803 getIptvInfo 方法的 adv.iptv.stballvlans 参数缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html |
| CNVD-2024-06236 | SAP LT Replication Server 授权问题漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html |
| CNVD-2024-06234 | Tenda AX1803 getIptvInfo 方法的 adv.iptv.stbpvid 参数缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/download/detail-3421.html |
| CNVD-2024-06246 | Tenda i29 pingSet 方法命令执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4916.html |
| CNVD-2024-06245 | Tenda i29 lanCfgSet 方法缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4916.html |
| CNVD-2024-06244 | Tenda i29 etPing 方法缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-4916.html |

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，获得提升的权限。此外，Apache、Fortinet、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞精心设计的 Web 应用程序 URL 伪造流量日志，通过高频发送特制的 HTTP 或 HTTPS 请求来执行拒绝服务攻击，通过特制的请求执行未经授权的代码或命令等。另外，Tenda AX1803 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞通过组件/goform/SetOnlineDevName 运行任意代码。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、SEMCMS SQL 注入漏洞（CNVD-2024-06232）

**验证描述**

SEMCMS 是一套支持多种语言的外贸网站内容管理系统（CMS）。

SEMCMS v4.8 版本存在 SQL 注入漏洞，该漏洞源于通过/web_inc.php 中的 languageID 参数缺少对外部输入 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://gitee.com/NoBlake/cve-2023-48864

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-06232

**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. 远控软件 AnyDesk 遭攻击致源代码和私钥被盗

远程桌面软件 AnyDesk 发布安全公告，确认其公司服务器遭到网络攻击，威胁攻击者窃取了部分源代码和代码签名密钥。

参考链接：https://www.secrss.com/articles/63478

### 2. 美国清洁用品巨头高乐氏因网络攻击损失 4900 万美元

高乐氏公司称去年 9 月的一次网络攻击迄今已造成该公司 4900 万美元的损失，高乐氏作为一家美国消费和专业清洁产品制造商，拥有 8700 名员工，2023 年收入近 75 亿美元。

参考链接：https://www.bleepingcomputer.com/news/security/clorox-says-cyberattack-caused-49-million-in-expenses/

**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