

## 信息安全漏洞周报

2023 年 12 月 11 日-2023 年 12 月 17 日

2023 年第 50 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 498 个，其中高危漏洞 234 个、中危漏洞 239 个、低危漏洞 25 个。漏洞平均分为 6.69。本周收录的漏洞中，涉及 0day 漏洞 392 个（占 79%），其中互联网上出现“BoidCMS 跨站脚本漏洞、JFinalCMS 跨站脚本漏洞（CNVD-2023-9773206）”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 45646 个，与上周（22289 个）环比增加 1.05 倍。

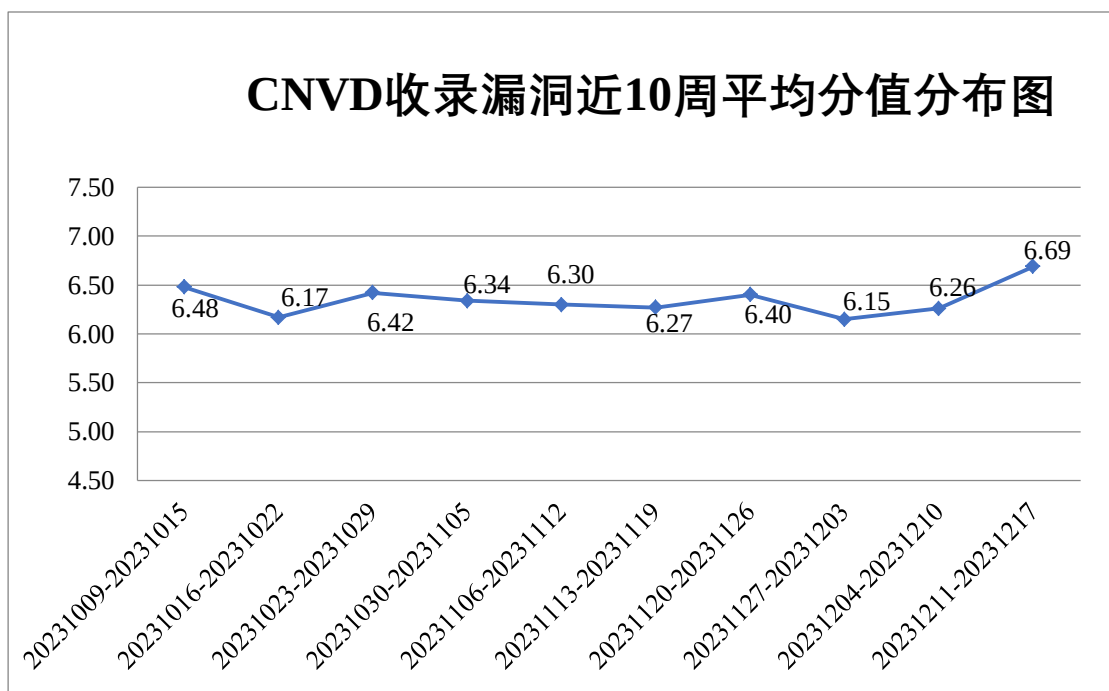


图 1 CNVD 收录漏洞近 10 周平均分分布图

### 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 10 起，向基础电

信企业通报漏洞事件 7 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 1230 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 224 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 27 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：

珠海金山办公软件有限公司、珠海海鸟科技有限公司、重庆软狐信息技术有限公司、重庆巨泰物联网集团有限公司、中控技术股份有限公司、中科软科技股份有限公司、智慧芽信息科技（苏州）有限公司、智互联（深圳）科技有限公司、郑州三晖电气股份有限公司、正文科技股份有限公司、正泰集团股份有限公司、浙江索颐科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江安邦护卫科技服务有限公司、长沙米拓信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、渔翁信息技术股份有限公司、友讯电子设备（上海）有限公司、优刻得科技股份有限公司、用友网络科技股份有限公司、炫米信息技术（上海）有限公司、夏普科技（上海）有限公司、武汉达梦数据库股份有限公司、威博通科技（上海）有限公司、网件（北京）网络技术有限公司、万兴科技集团股份有限公司、天津市神州商龙科技股份有限公司、腾讯安全应急响应中心、随锐科技集团股份有限公司、速达软件技术（广州）有限公司、苏州万户网络科技有限公司、苏州欧姆尼克新能源科技有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、深圳坐标软件集团有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市优卡特电子有限公司、深圳市万人市场调查股份有限公司、深圳市蓝凌软件股份有限公司、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、深圳市泓源林计算机软件有限公司、深圳市博实结科技股份有限公司、深圳市昂捷信息技术股份有限公司、深圳奥哲网络科技有限公司、上海卓卓网络科技有限公司、上海智引信息科技有限公司、上海甄云科技信息有限公司、上海真兰仪表科技股份有限公司、上海远丰信息科技（集团）有限公司、上海翊谱信息科技有限公司、上海万欣计算机信息科技有限公司、上海天旦网络科技有限公司、上海荃路软件开发工作室、上海皆唯软件科技有限公司、上海建文软件有限公司、上海技腾通讯设备有限公司、上海华测导航技术股份有限公司、上海海鼎信息工程股份有限公司、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、上海必智科技有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、商派软件有限公司、陕西小伙伴网络科技有限公司、陕西卡一车物流科技有限公司、山东云时空信息科技有限公司、山东影响力智能科技有限公司、山东潍微科技股份有限公司、山东绿创智能科技有限公司、山东博硕自动化技术有限公司、厦门四信通信科技有限公司、厦门目享网络科技有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、任子行网络技术股份有限公司、青岛东软载波科技股份有限公司、品茗科技股份有限公司、鹏为软件股份有限公司、配配通（上海）贸易服

务有限公司、内蒙古包钢钢联物流有限公司、南京中新赛克科技有限责任公司、南京科远智慧科技集团股份有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、联想（北京）有限公司、蓝网科技股份有限公司、昆仑万维科技股份有限公司、金卡银证软件（杭州）有限公司、金蝶软件（中国）有限公司、江西志浩电子科技有限公司、江西博微新技术有限公司、江苏圃惠汇达通讯设备有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖州蜗牛网络科技有限公司、湖南强智科技发展有限公司、湖南华美信息系统有限公司、洪湖尔创网联信息技术有限公司、红盛集团（深圳）有限公司、河北欧润天腾云梦吧网络工作室、杭州易软共创网络科技有限公司、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、杭州恩软信息技术有限公司、海宁市车辆停泊开发服务有限公司、国泰新点软件股份有限公司、广州盈可视电子科技有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广州市奥威亚电子科技有限公司、广州全通数码科技有限公司、广州青鹿教育科技有限公司、广州红帆科技有限公司、广州安网通信技术有限公司、广西海豚有海信息科技有限公司、广联达科技股份有限公司、广东伟达智能装备股份有限公司、广东泰恪网络科技有限公司、广东世纪信通科技股份有限公司、富士胶片（中国）投资有限公司、福州联讯信息科技有限公司、福建银达汇智信息科技股份有限公司、福建博思软件股份有限公司、烽火通信科技股份有限公司、东华医为科技有限公司、东华软件股份公司、东莞市通天星软件科技有限公司、成都生动网络科技有限公司、成都飞鱼星科技股份有限公司、成都成电医星数字健康软件有限公司、超威半导体产品（中国）有限公司、常州天健智能科技有限公司、北京中农信达信息技术有限公司、北京长亭科技有限公司、北京亿赛通科技发展有限责任公司、北京兴辅科技有限公司、北京星网锐捷网络技术有限公司、北京威努特技术有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京世纪超星信息技术发展有限责任公司、北京旷视科技有限公司、北京金万维科技有限公司、北京金盘鹏图软件技术有限公司、北京金和网络股份有限公司、北京慧图科技（集团）股份有限公司、北京宏景世纪软件股份有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、北京安领可信网络科技有限公司、北京爱奇艺科技有限公司、安徽中技国医医疗科技有限公司、安徽皖通邮电股份有限公司、安徽青柿信息科技有限公司和爱普生（中国）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，天津市国瑞数码安全系统股份有限公司、新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。中孚安全技术有限公司、江苏金盾

检测技术股份有限公司、浙江安腾信息技术有限公司、杭州默安科技有限公司、联想集团、贵州多彩网安科技有限公司、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、快页信息技术有限公司、安徽锋刃信息科技有限公司、亚信科技（成都）有限公司、安徽天行网安信息安全技术有限公司、江苏百达智慧网络科技有限公司、星云博创科技有限公司、统信软件技术有限公司、赛尔网络有限公司、上海谋乐网络科技有限公司、南京共美科技有限公司、江苏晟晖信息科技有限公司、北京天防安全科技有限公司、北京山石网科信息技术有限公司、智网安云（武汉）信息技术有限公司、山石网科通信技术股份有限公司、信息产业信息安全测评中心、北京微步在线科技有限公司、成都安美勤信息技术股份有限公司、河南灵创电子科技有限公司、江苏极元信息技术有限公司、中国工商银行、博智安全科技股份有限公司、成都卓越华安信息技术服务有限公司、广州安亿信软件科技有限公司、信联科技（南京）有限公司、上海市信息安全测评认证中心、河南悦海数安科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、深圳昂楷科技有限公司、合肥梆梆信息科技有限公司、浙江国利网安科技有限公司、江苏易安联网络技术有限公司、山东正中信息技术股份有限公司、中科国宏科技有限公司、北京双湃智安科技有限公司、杭州智顺科技有限公司、成方金融科技有限公司上海分公司、河南天祺信息安全技术有限公司、苏州棱镜七彩信息科技有限公司、河北镌远网络科技有限公司、杭州安信检测技术有限公司、上海直画科技有限公司、江西诚韬科技有限公司、西藏熙安信息技术有限责任公司及其他个人白帽子向 CNVD 提交了 45646 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 43583 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）        | 24861  | 24861 |
| 奇安信网神（补天平台）       | 17964  | 17964 |
| 天津市国瑞数码安全系统股份有限公司 | 2570   | 0     |
| 新华三技术有限公司         | 736    | 0     |
| 三六零数字安全科技集团有限公司   | 558    | 558   |
| 深信服科技股份有限公司       | 436    | 2     |
| 安天科技集团股份有限公司      | 297    | 0     |

|                      |     |     |
|----------------------|-----|-----|
| 北京数字观星科技有限公司         | 281 | 0   |
| 上海交大                 | 200 | 200 |
| 北京神州绿盟科技有限公司         | 138 | 0   |
| 北京启明星辰信息安全技术有限公司     | 95  | 9   |
| 北京知道创宇信息技术有限公司       | 76  | 0   |
| 远江盛邦（北京）网络安全科技股份有限公司 | 59  | 59  |
| 北京天融信网络安全技术有限公司      | 34  | 9   |
| 北京安信天行科技有限公司         | 24  | 24  |
| 阿里云计算有限公司            | 10  | 10  |
| 杭州迪普科技股份有限公司         | 10  | 0   |
| 北京智游网安科技有限公司         | 5   | 5   |
| 北京长亭科技有限公司           | 3   | 3   |
| 中电科网络安全科技股份有限公司      | 3   | 3   |
| 华为技术有限公司             | 2   | 2   |
| 北京升鑫网络科技有限公司（青藤云）    | 1   | 1   |
| 杭州安恒信息技术股份有限公司       | 1   | 1   |
| 中孚安全技术有限公司           | 163 | 163 |
| 江苏金盾检测技术股份有限公司       | 59  | 59  |
| 浙江安腾信息技术有            | 36  | 36  |

|                  |    |    |
|------------------|----|----|
| 限公司              |    |    |
| 杭州默安科技有限公司       | 35 | 35 |
| 联想集团             | 30 | 30 |
| 贵州多彩网安科技有限公司     | 24 | 24 |
| 河南东方云盾信息技术有限公司   | 23 | 23 |
| 内蒙古洞明科技有限公司      | 22 | 22 |
| 快页信息技术有限公司       | 21 | 21 |
| 西门子（中国）有限公司      | 18 | 0  |
| 安徽锋刃信息科技有限公司     | 15 | 15 |
| 亚信科技（成都）有限公司     | 14 | 14 |
| 安徽天行网安信息安全技术有限公司 | 11 | 11 |
| 江苏百达智慧网络科技有限公司   | 11 | 11 |
| 星云博创科技有限公司       | 6  | 6  |
| 统信软件技术有限公司       | 5  | 5  |
| 赛尔网络有限公司         | 5  | 5  |
| 上海谋乐网络科技有限公司     | 5  | 5  |
| 南京共美科技有限公司       | 4  | 4  |
| 江苏晟晖信息科技有限公司     | 3  | 3  |
| 北京天防安全科技有限公司     | 3  | 3  |

|                      |   |   |
|----------------------|---|---|
| 北京山石网科信息技术有限公司       | 3 | 3 |
| 智网安云（武汉）信息技术有限公司     | 3 | 3 |
| 山石网科通信技术股份有限公司       | 3 | 3 |
| 信息产业信息安全测评中心         | 3 | 3 |
| 北京微步在线科技有限公司         | 2 | 2 |
| 成都安美勤信息技术股份有限公司      | 2 | 2 |
| 河南灵创电子科技有限公司         | 2 | 2 |
| 江苏极元信息技术有限公司         | 2 | 2 |
| 中国工商银行               | 2 | 2 |
| 博智安全科技股份有限公司         | 2 | 2 |
| 成都卓越华安信息技术服务有限公司     | 1 | 1 |
| 广州安亿信软件科技有限公司        | 1 | 1 |
| 信联科技（南京）有限公司         | 1 | 1 |
| 上海市信息安全测评认证中心        | 1 | 1 |
| 河南悦海数安科技有限公司         | 1 | 1 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 1 | 1 |
| 深圳昂楷科技有限公司           | 1 | 1 |
| 合肥梆梆信息科技有限公司         | 1 | 1 |

|                     |       |       |
|---------------------|-------|-------|
| 限公司                 |       |       |
| 浙江国利网安科技有<br>限公司    | 1     | 1     |
| 江苏易安联网络技术<br>有限公司   | 1     | 1     |
| 山东正中信息技术股<br>份有限公司  | 1     | 1     |
| 中科国宏科技有限公<br>司      | 1     | 1     |
| 北京双湃智安科技有<br>限公司    | 1     | 1     |
| 杭州智顺科技有限公<br>司      | 1     | 1     |
| 成方金融科技有限公<br>司上海分公司 | 1     | 1     |
| 河南天祺信息安全技<br>术有限公司  | 1     | 1     |
| 苏州棱镜七彩信息科<br>技有限公司  | 1     | 1     |
| 河北镌远网络科技有<br>限公司    | 1     | 1     |
| 杭州安信检测技术有<br>限公司    | 1     | 1     |
| 上海直画科技有限公<br>司      | 1     | 1     |
| 江西诚韬科技有限公<br>司      | 1     | 1     |
| 西藏熙安信息技术有<br>限责任公司  | 1     | 1     |
| CNCERT 广西分中心        | 7     | 7     |
| 个人                  | 1387  | 1387  |
| 报送总计                | 50317 | 45646 |

本周，CNVD 收录了 498 个漏洞。WEB 应用 234 个，应用程序 99 个，网络设备（交换机、路由器等网络端设备）97 个，操作系统 36 个，智能设备（物联网终端设备）24 个，安全产品 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              | 234  |
| 应用程序                | 99   |
| 网络设备（交换机、路由器等网络端设备） | 97   |
| 操作系统                | 36   |
| 智能设备（物联网终端设备）       | 24   |
| 安全产品                | 8    |

本周CNVD漏洞数量按影响类型分布

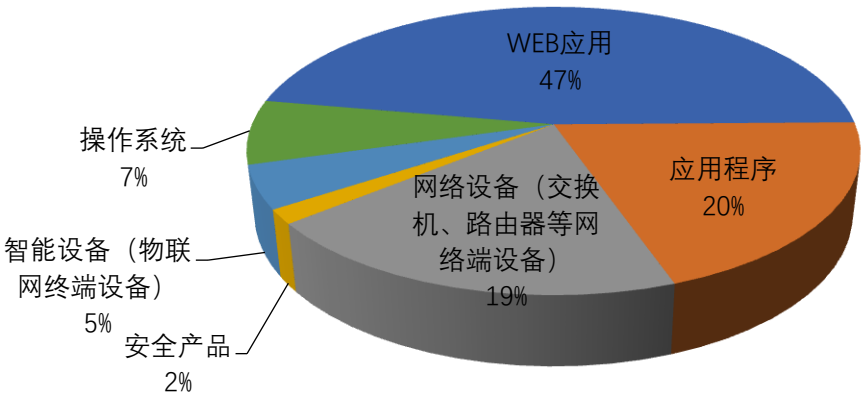


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、用友网络科技股份有限公司、Siemens 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       | 31   | 6%   |
| 2  | 用友网络科技股份有限公司 | 23   | 5%   |
| 3  | Siemens      | 19   | 4%   |
| 4  | Tenda        | 14   | 3%   |

|    |                |     |     |
|----|----------------|-----|-----|
| 5  | 北京星网锐捷网络技术有限公司 | 13  | 3%  |
| 6  | Apache         | 12  | 3%  |
| 7  | D-Link         | 11  | 2%  |
| 8  | DELL           | 10  | 1%  |
| 9  | FreeImage      | 7   | 1%  |
| 10 | 其他             | 358 | 72% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 69 个电信行业漏洞，63 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Siemens User Management Component (UMC)经典缓冲区溢出漏洞、Bosch Ethernet switch PRA-ES8P2S Web 接口 diagnostics 命令执行漏洞”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/>

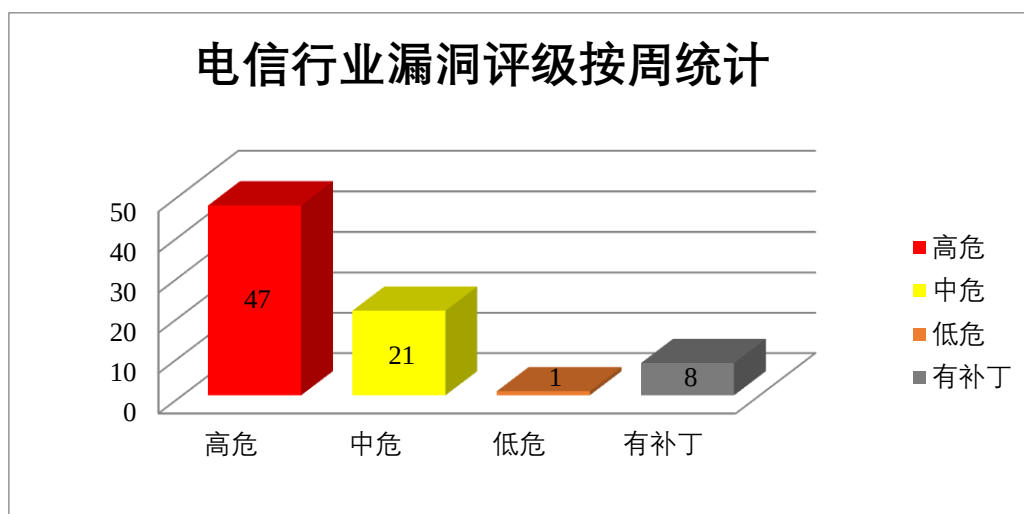


图 3 电信行业漏洞统计

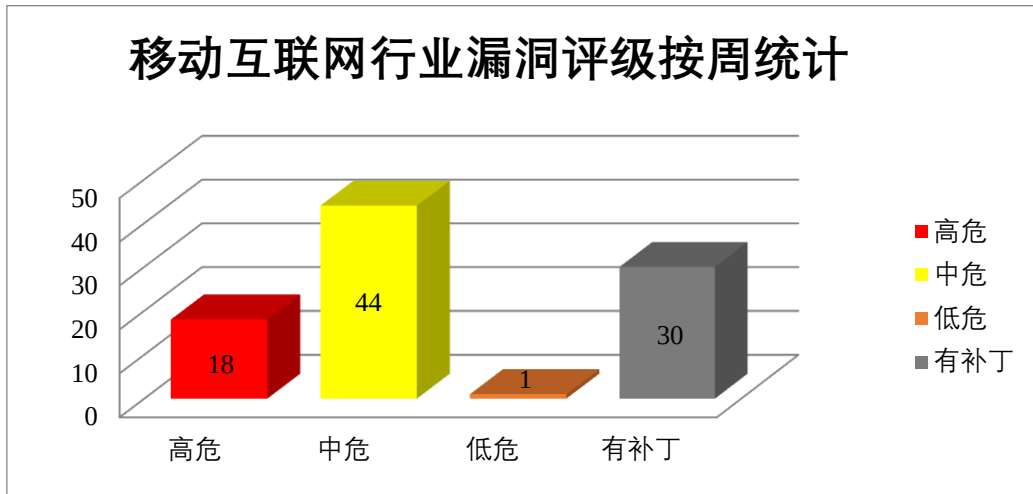


图 4 移动互联网行业漏洞统计

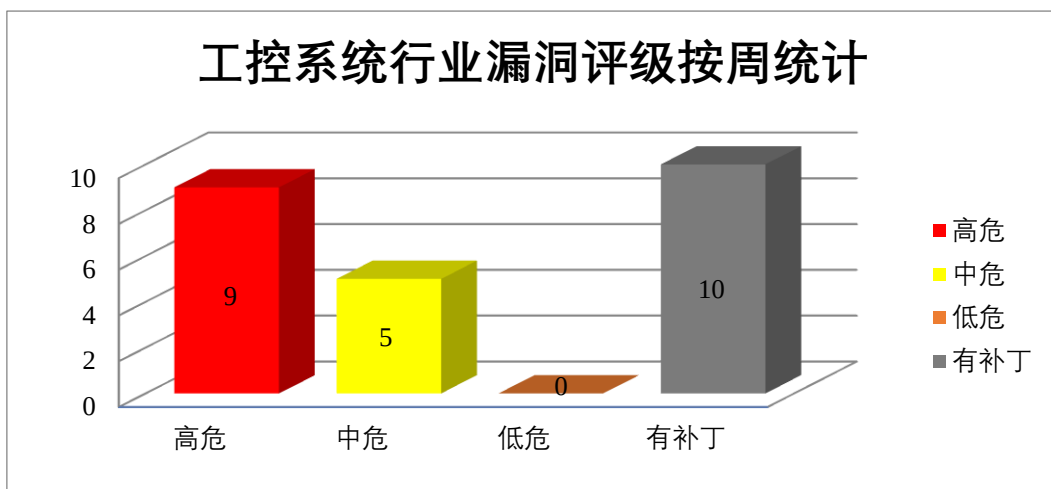


图 5 工控系统行业漏洞统计

## 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、DELL 产品安全漏洞

Dell DM5500 是美国戴尔（Dell）公司的一款集成解决方案。提供业界领先的重复数据删除、数据保护解决方案和多云功能。Dell PowerScale OneFS 是一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞覆盖服务器文件系统上存储的文件，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Dell DM5500 权限提升漏洞、Dell DM5500 身份验证错误漏洞、Dell DM5500 操作系统命令注入漏洞、Dell DM5500 路径遍历漏洞、Dell DM5500 跨站脚本漏洞、Dell DM5500 缓冲区溢出漏洞、Dell PowerScale OneFS 拒绝服务漏洞（CNVD-2023-9671099）、Dell DM5500 信息泄露漏洞。其中，除“Dell DM 5500 跨站脚本漏洞、Dell DM5500 信息泄露漏洞”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-2023-96703>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96708>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96707>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96706>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96705>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96704>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96710>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96709>

## 2、Apache 产品安全漏洞

Apache Cocoon 是美国阿帕奇（Apache）基金会的一个基于组件的 Web 开发的概念构建的 Web 应用程序框架。Apache Superset 是一个数据可视化和数据探索平台。Apache Submarine 是云原生机器学习平台。Apache UIMA 是一个组件化的软件架构。用于分析同终端用户相关联的大容量非结构化信息。Apache Struts 是一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。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发送特制的 XML 文件读取文件，窃取数据库敏感数据，导致代码执行等。

CNVD 收录的相关漏洞包括：Apache Cocoon XML 外部实体注入漏洞、Apache Cocoon SQL 注入漏洞、Apache Superset 跨站脚本漏洞（CNVD-2023-9665948）、Apache Superset 输入验证错误漏洞（CNVD-2023-9666130）、Apache Superset 授权问题漏洞（CNVD-2023-9666047）、Apache Submarine 反序列化漏洞、Apache UIMA 反序列化漏洞、Apache Struts 目录遍历漏洞。其中，除“Apache Superset 跨站脚本漏洞（CNVD-2023-9665948）、Apache Superset 输入验证错误漏洞（CNVD-2023-9666130）、Apache Superset 授权问题漏洞（CNVD-2023-9666047）”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-2023-96657>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96656>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96659>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96661>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96660>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96664>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96665>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97016>

### 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，攻击者可利用漏洞在系统上执行任意代码，导致权限提升。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-96682、CNVD-2023-96681、CNVD-2023-96680、CNVD-2023-96685、CNVD-2023-96684、CNVD-2023-96683、CNVD-2023-96689）、Google Android 代码执行漏洞（CNVD-2023-96686）。其中，“Google Android 代码执行漏洞（CNVD-2023-96686）”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-2023-96682>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96681>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96680>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96686>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96685>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96684>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96683>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-96689>

### 4、Siemens 产品安全漏洞

SCALANCE M-800、MUM-800 和 S615 以及 RUGGEDCOM RM1224 都是工业路由器。SINEC INS（基础设施网络服务）是一个基于 web 的应用程序，将各种网络服务结合在一个工具中。这简化了与工业网络相关的所有网络服务的安装和管理。SIMATIC PC Station 是一个软件组件，用于管理 PC 上的 SIMATIC 软件产品和接口。SIMATIC S7-400 控制器专为工业环境中的离散和连续控制而设计，如世界各地的制造业、食品和饮料以及化工行业。SIMATIC CP 1242 和 CP 1243 相关处理器将 SIMATIC S7-1200 控制器连接到广域网（WAN）。它们提供集成的安全功能，如防火墙、虚拟专用网络（VPN）以及对其他数据加密协议的支持。SIMATIC CP 1543-1 通信处理器将 SIMATIC S7-1500 控制器连接到以太网。它们提供集成的安全功能，如防火墙、虚拟专用网络（VPN）以及对其他数据加密协议的支持。SINUMERIK MC 是一个用于定制机器解决方案的 CNC 系统。SINUMERIK ONE 是一个数字原生数控系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞截获发送到 UMC 服务器的凭据，并操纵响应，从而升级权限，在系统上执行命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens SINEC INS 操作系统命令注入漏洞、Siemens SCALANCE M-800/S615 系列操作系统命令注入漏洞（CNVD-2023-97257、CNVD-2023-97258）、Siemens SINEC INS 证书验证不当漏洞、Siemens 多款产品 Web 服务器

拒绝服务漏洞（CNVD-2023-97269、CNVD-2023-97270）、Siemens 工业产品 Web 服务器拒绝服务漏洞、Siemens SINUMERIK ONE 和 SINUMERIK-MC 拒绝服务漏洞。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-2023-97255>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97257>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97256>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97258>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97269>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97270>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97273>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-97274>

5、Tenda AX3 命令执行漏洞

Tenda Ax3 是中国腾达（Tenda）公司的一款 Ax1800 千兆端口双频 Wifi 6 无线路由器。本周，Tenda AX3 被披露存在命令执行漏洞。攻击者可利用该漏洞导致任意命令执行。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-2023-98044>

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-2023-96656 | Apache Cocoon SQL 注入漏洞  | 高    | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="https://lists.apache.org/thread/lsvd1hmr2t2q823x21d5ygzgbj9jpvjp">https://lists.apache.org/thread/lsvd1hmr2t2q823x21d5ygzgbj9jpvjp</a>                                                                                                                                                                                                 |
| CNVD-2023-96664 | Apache Submarine 反序列化漏洞 | 高    | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="https://github.com/apache/submarine/pull/1054">https://github.com/apache/submarine/pull/1054</a>                                                                                                                                                                                                                                       |
| CNVD-2023-96703 | Dell DM5500 权限提升漏洞      | 高    | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="https://www.dell.com/support/kbdoc/en-us/000220107/dsa-2023-425-security-update-for-dell-powerprotect-data-manager-dm5500-appliance-for-multiple-vulnerabilities">https://www.dell.com/support/kbdoc/en-us/000220107/dsa-2023-425-security-update-for-dell-powerprotect-data-manager-dm5500-appliance-for-multiple-vulnerabilities</a> |
| CNVD-2023-97250 | 多款 Cisco 产品代码注入漏洞       | 高    | 厂商已发布了漏洞修复程序，请及时关注更新：                                                                                                                                                                                                                                                                                                                                                    |

|                 |                                                                    |   |                                                                                                                                                                                                                         |
|-----------------|--------------------------------------------------------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                                                    |   | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm</a> |
| CNVD-2023-97275 | Siemens User Management Component (UMC)经典缓冲区溢出漏洞 (CNVD-2023-97275) | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="https://cert-portal.siemens.com/productcert/html/ssa-999588.html">https://cert-portal.siemens.com/productcert/html/ssa-999588.html</a>                                             |
| CNVD-2023-97279 | Siemens User Management Component (UMC)输入验证不当漏洞                    | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="https://cert-portal.siemens.com/productcert/html/ssa-999588.html">https://cert-portal.siemens.com/productcert/html/ssa-999588.html</a>                                             |
| CNVD-2023-97499 | PrestaShop SQL 注入漏洞 (CNVD-2023-9749945)                            | 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：<br><a href="https://security.friendsofpresta.org/modules/2023/11/28/ticons.html">https://security.friendsofpresta.org/modules/2023/11/28/ticons.html</a>                              |
| CNVD-2023-97500 | Squid 缓冲区溢出漏洞 (CNVD-2023-9750097)                                  | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="http://www.squid-cache.org/Versions/v6/SQUID-2023_7.patch">http://www.squid-cache.org/Versions/v6/SQUID-2023_7.patch</a>                                                              |
| CNVD-2023-97826 | Zammad 访问控制错误漏洞 (CNVD-2023-9782629)                                | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="https://zammad.com/en/advisories/zaa-2023-06">https://zammad.com/en/advisories/zaa-2023-06</a>                                                                                        |
| CNVD-2023-98158 | osCommerce SQL 注入漏洞                                                | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：<br><a href="https://www.oscommerce.com/download-oscommerce">https://www.oscommerce.com/download-oscommerce</a>                                                                                    |

小结：本周，DELL 产品被披露存在多个漏洞，攻击者可利用漏洞覆盖服务器文件系统上存储的文件，执行任意代码，导致拒绝服务等。此外，Apache、Google、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过发送特制的 XML 文件读取文件，在系统上执行任意代码，导致权限提升，拒绝服务等。另外，Tenda AX3 被披露存在命令执行漏洞。攻击者可利用漏洞导致任意命令执行。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、JFinalCMS 跨站脚本漏洞 (CNVD-2023-97732)

#### 验证描述

JFinalCMS 是一个内容管理系统。

JFinalCMS 存在跨站脚本漏洞，该漏洞源于在模型管理部门对用户提供的数据库数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

### 验证信息

POC 链接: <https://github.com/Rabb1ter/cms/blob/main/There%20is%20a%20stored%20XSS%20in%20the%20model%20management%20department.md>

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2023-97732>

### 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 Struts 2 曝出远程代码执行漏洞

近日，阿帕奇公司发布安全公告称 Struts 2 开源 Web 应用程序框架存在安全漏洞，可能导致远程代码执行。

参考链接: <https://www.freebuf.com/news/386423.html>

### 2. WordPress 插件曝出安全漏洞，导致 5 万个网站遭受 RCE 攻击

一个安装了超过 9 万次的 WordPress 插件中存在一个安全漏洞，威胁攻击者能够利用该漏洞获得远程代码执行权限。

参考链接: <https://www.bleepingcomputer.com/news/security/50k-wordpress-sites-exposed-to-rce-attacks-by-critical-bug-in-backup-plugin/>

## 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](http://www.cert.org.cn)

邮箱: [vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话: 010-82991537