# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2024 年 10 月 14 日-2021 年 10 月 20 日** **2024 年第 42 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 272 个，其中高危漏洞 151 个、中危漏洞 106 个、低危漏洞 15 个。漏洞平均分值为 6.76。本周收录的漏洞中，涉及 0day 漏洞 183 个（占 67%），其中互联网上出现“Ellevo 跨站脚本漏洞、Tenda G3 缓冲区溢出漏洞（CNVD-2024-40839）”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 5533 个，与上周（9281 个）环比减少 40%。

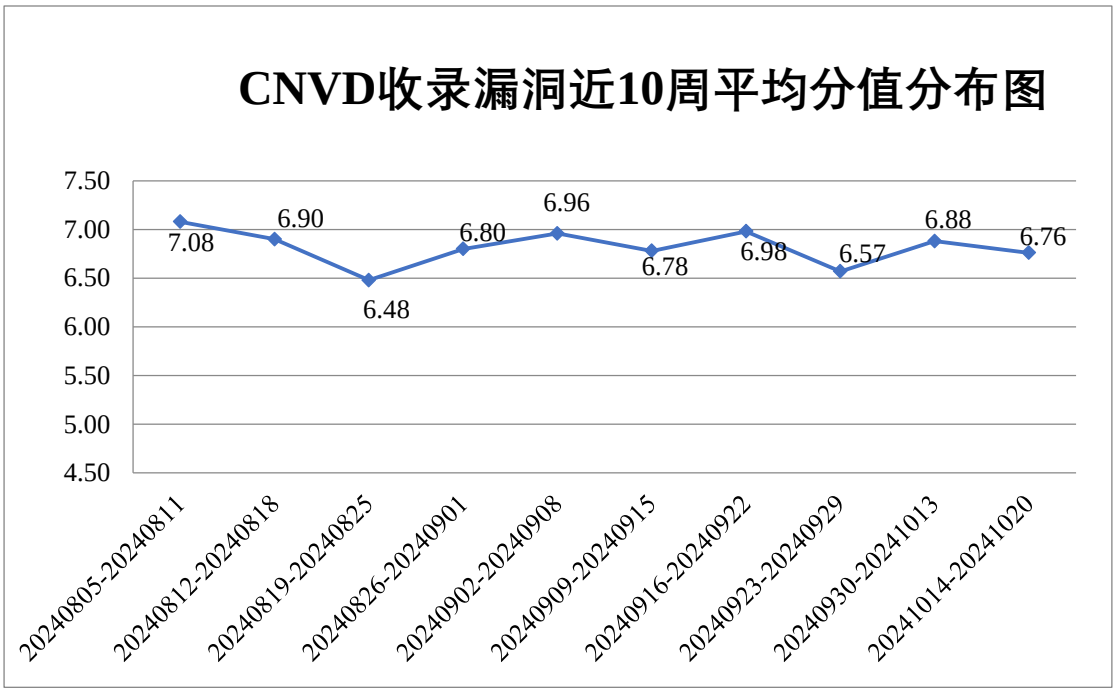


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 10 起，向基础电

信企业通报漏洞事件 3 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 377 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 45 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 12 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：

重庆朗奕迪实业有限公司、中控技术股份有限公司、中科数字通（北京）科技有限公司、中建材信云智联科技有限公司、智互联（深圳）科技有限公司、长沙友点软件科技有限公司、枣庄市亿景计算机科技有限公司、友讯电子设备（上海）有限公司、优慕课在线教育科技（北京）有限责任公司、用友网络科技股份有限公司、新天科技股份有限公司、新道科技股份有限公司、西安瑞友信息技术资讯有限公司、武汉天地伟业科技有限公司、武汉金同方科技有限公司、武汉达梦数据库有限公司、网隆云计算有限公司、太原迅易科技有限公司、苏州汇川技术有限公司、苏州汇成软件开发科技有限公司、深圳坐标软件集团有限公司、深圳维盟网络技术有限公司、深圳市思迅软件股份有限公司、深圳市蓝凌软件股份有限公司、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、深圳市红门智慧停车科技有限公司、深圳市东宝信息技术有限公司、深圳市潮流网络技术有限公司、深圳市必联电子有限公司、深圳迈贝尔科技有限公司、深圳奥联信息安全技术有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海桑锐电子科技股份有限公司、上海灵当信息科技有限公司、上海寰创通信科技股份有限公司、上海泛微网络科技股份有限公司、上海得帆信息技术有限公司、上海博达数据通信有限公司、上海冰峰计算机网络技术有限公司、上海百胜软件股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山石网科通信技术（北京）有限公司、山东点狮信息科技有限公司、山东比特智能科技股份有限公司、厦门科拓通讯技术股份有限公司、赛蓝（广州）信息技术有限公司、润申信息科技(上海)有限公司、瑞斯康达科技发展股份有限公司、确信信息股份有限公司、青果软件集团有限公司、青岛和正信息技术有限公司、青岛东胜伟业软件有限公司、青岛东软载波科技股份有限公司、青创未来集团有限公司、麒麟软件有限公司、普联技术有限公司、品茗科技股份有限公司、南京明德软件有限公司、摩莎科技（上海）有限公司、麦克奥迪实业集团有限公司、迈普通信技术股份有限公司、罗格朗（上海）管理有限公司、龙泉驿区梦缘计算机经营部、辽宁成创网络科技有限公司、联想安全实验室、蓝网科技股份有限公司、科华数据股份有限公司、柯尼卡美能达集团、京瓷办公信息系统（中国）有限公司、捷普电子（无锡）有限公司、江苏金智科技股份有限公司、慧与（中国）有限公司、华硕电脑（上海）有限公司、华平信息技术股份有限公司、红门智能科技股份有限公司、河南吉海网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、哈尔滨新中新电子股份有限公司、桂林市国投数据科技发展有限公司、桂林佳朋信息科技有

限公司、贵州小码科技有限公司、广州协众软件科技有限公司、广州同聚成电子科技有限公司、广州璐华信息技术有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、固德威技术股份有限公司、东莞市同享软件科技有限公司、东北师大理想软件股份有限公司、鼎点视讯科技有限公司、大连爱智控制系统有限公司、承德博冠实业集团有限公司、成都星锐蓝海网络科技有限公司、成都索贝数码科技股份有限公司、畅捷通信息技术股份有限公司、畅畅行网络科技有限公司、常州红金羚软件技术有限公司、北京中控科技发展有限公司、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、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京山石网科信息技术有限公司、北京美特软件技术有限公司、北京猎鹰安全科技有限公司、北京金万维科技有限公司、北京金和网络股份有限公司、北京广通优云科技股份有限公司、北京北大方正电子有限公司、北京宝兰德软件股份有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安吉加加信息技术有限公司、安徽旭帆信息科技有限公司、安徽生命港湾信息技术有限公司、安徽容知日新科技股份有限公司、安徽科迅教育装备集团有限公司和爱普生（中国）有限公司。

本周，CNVD 发布了《Oracle 发布 2024 年 10 月的安全公告》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10511）。

## 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、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、北京升鑫网络科技有限公司（青藤云）等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、中孚安全技术有限公司、江苏金盾检测技术股份有限公司、北京翰慧投资咨询有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、北京中睿天下信息技术有限公司、河南灵创电子科技有限公司、江苏耘和计算机系统工程有限公司、苏州棱镜七彩信息科技有限公司、上海谋乐网络科技有限公司、联通数字科技有限公司、北京网御星云信息技术有限公司、江苏云天网络安全技术有限公司、上海观安信息技术股份有限公司、北京大学、北京航空航天大学、星舟有信（北京）信息技术有限公司、杭州海康威视数字技术股份有限公司、中资网络信息安全科技有限公司、安徽天行网安信息安全技术有限公司、长春市安山中龙计算机技术有限公司、北京卓识网安技术股份有限公司、北京微步在线科技有限公司、中电福富信息科技有限公司、中华人民共和国广东海事局、成都安美勤信息技术股份有限公司、广东粤密技术服务有限公司、中国工商银行、天翼数字生活科技有限公司、国网信息通信产业集团有限公司、北京山石网科信息技术有限

公司、任子行网络技术股份有限公司、成都久信信息技术股份有限公司、南方电网科学研究院有限责任公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 5533 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和上海交大向 CNVD 共享的白帽子报送的 3249 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 | 原创漏洞数量 |
| --- | --- | --- |
| 斗象科技（漏洞盒子） | 2468 | 2468 |
| 新华三技术有限公司 | 804 | 0 |
| 深信服科技股份有限公司 | 578 | 32 |
| 上海交大 | 461 | 461 |
| 北京神州绿盟科技有限公司 | 386 | 252 |
| 北京数字观星科技有限公司 | 338 | 0 |
| 三六零数字安全科技集团有限公司 | 320 | 320 |
| 北京升鑫网络科技有限公司（青藤云） | 166 | 166 |
| 阿里云计算有限公司 | 165 | 0 |
| 北京知道创宇信息技术有限公司 | 153 | 3 |
| 华为技术有限公司 | 94 | 22 |
| 恒安嘉新（北京）科技股份公司 | 89 | 0 |
| 杭州安恒信息技术股份有限公司 | 82 | 82 |
| 北京启明星辰信息安全技术有限公司 | 68 | 4 |
| 北京长亭科技有限公司 | 33 | 3 |
| 南京众智维信息科技有限公司 | 33 | 15 |
| 杭州迪普科技股份有 | 12 | 2 |

| | | |
|---|---|---|
| 限公司 | | |
| 北京天融信网络安全技术有限公司 | 7 | 7 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 7 | 7 |
| 北京智游网安科技有限公司 | 2 | 2 |
| 北京安信天行科技有限公司 | 1 | 1 |
| 京东科技信息技术有限公司 | 1 | 1 |
| 北京云科安信科技有限公司 | 1 | 1 |
| 成都卫士通信息安全技术有限公司 | 339 | 339 |
| 中孚安全技术有限公司 | 133 | 133 |
| 江苏金盾检测技术股份有限公司 | 37 | 37 |
| 北京翰慧投资咨询有限公司 | 36 | 36 |
| 河南东方云盾信息技术有限公司 | 23 | 23 |
| 快页信息技术有限公司 | 20 | 20 |
| 北京中睿天下信息技术有限公司 | 8 | 8 |
| 河南灵创电子科技有限公司 | 8 | 8 |
| 江苏耘和计算机系统工程有限公司 | 8 | 8 |
| 苏州棱镜七彩信息科技有限公司 | 7 | 7 |
| 上海谋乐网络科技有 | 6 | 6 |

| | | |
|---|---|---|
| 限公司 | | |
| 联通数字科技有限公司 | 6 | 6 |
| 北京网御星云信息技术有限公司 | 6 | 6 |
| 江苏云天网络安全技术有限公司 | 5 | 5 |
| 上海观安信息技术股份有限公司 | 5 | 5 |
| 北京大学 | 5 | 5 |
| 北京航空航天大学 | 4 | 4 |
| 星舟有信（北京）信息技术有限公司 | 4 | 4 |
| 杭州海康威视数字技术股份有限公司 | 3 | 3 |
| 中资网络信息安全科技有限公司 | 3 | 3 |
| 安徽天行网安信息安全技术有限公司 | 3 | 3 |
| 长春市安山中龙计算机技术有限公司 | 2 | 2 |
| 北京卓识网安技术股份有限公司 | 2 | 2 |
| 北京微步在线科技有限公司 | 2 | 2 |
| 中电福富信息科技有限公司 | 2 | 2 |
| 中华人民共和国广东海事局 | 2 | 2 |
| 成都安美勤信息技术股份有限公司 | 2 | 2 |
| 广东粤密技术服务有限公司 | 1 | 1 |
| 中国工商银行 | 1 | 1 |
| 天翼数字生活科技有 | 1 | 1 |

| | | |
|---|---|---|
| 限公司 | | |
| 国网信息通信产业集团有限公司 | 1 | 1 |
| 北京山石网科信息技术有限公司 | 1 | 1 |
| 任子行网络技术股份有限公司 | 1 | 1 |
| 成都久信信息技术股份有限公司 | 1 | 1 |
| 南方电网科学研究院有限责任公司 | 1 | 1 |
| 山石网科通信技术股份有限公司 | 1 | 1 |
| CNCERT 宁夏分中心 | 10 | 10 |
| CNCERT 河北分中心 | 2 | 2 |
| CNCERT 北京分中心 | 1 | 1 |
| CNCERT 福建分中心 | 1 | 1 |
| 个人 | 980 | 980 |
| 报送总计 | 7953 | 5533 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 272 个漏洞。WEB 应用 122 个，应用程序 69 个，网络设备（交换机、路由器等网络端设备）48 个，安全产品 17 个，智能设备（物联网终端设备）11 个，数据库 2 个，区块链公链 2 个，操作系统 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 | 122 |
| 应用程序 | 69 |
| 网络设备（交换机、路由器等网络端设备） | 48 |
| 安全产品 | 17 |
| 智能设备（物联网终端设备） | 11 |
| 数据库 | 2 |
| 区块链公链 | 2 |
| 操作系统 | 1 |

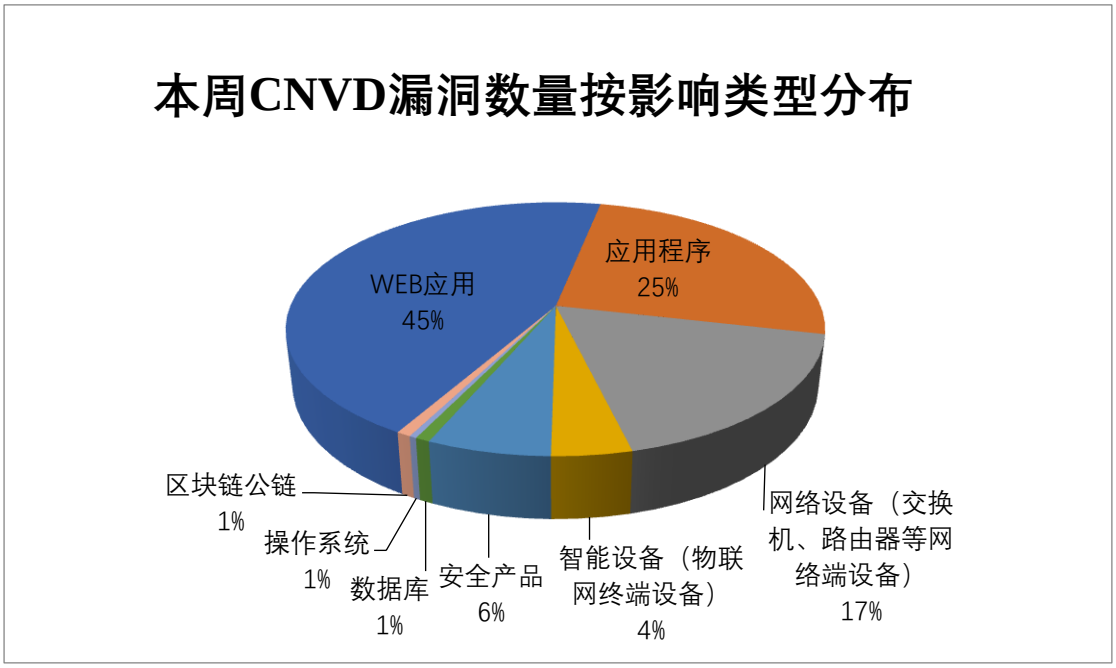


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、esri、PDF-XChange 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 | D-Link | 18 | 7% |
| 2 | esri | 11 | 4% |
| 3 | PDF-XChange | 11 | 4% |
| 4 | Adobe | 10 | 4% |
| 5 | Trend Micro | 10 | 4% |
| 6 | 畅捷通信息技术股份有限公司 | 9 | 3% |
| 7 | Microsoft | 9 | 3% |
| 8 | Foxit | 8 | 3% |
| 9 | 安美世纪（北京）科技有限公司 | 8 | 3% |
| 10 | 其他 | 178 | 65% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，3 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“Delta Electronics CNCSoft-G2 缓冲区溢出漏洞（CNVD-2024-40829）、Rockwell Automation Pavilion8 授权问题漏洞（CNVD-2024-40835）”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/

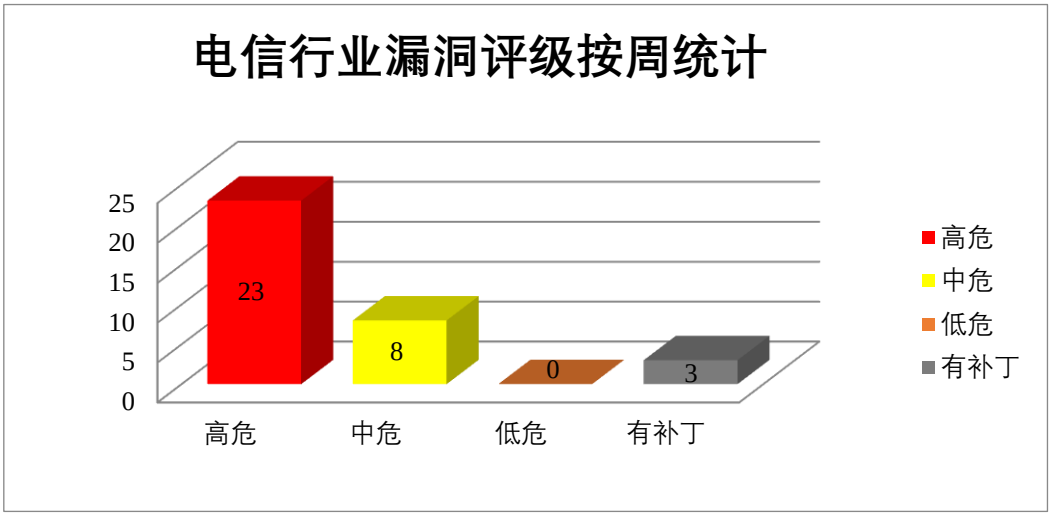


图 3 电信行业漏洞统计

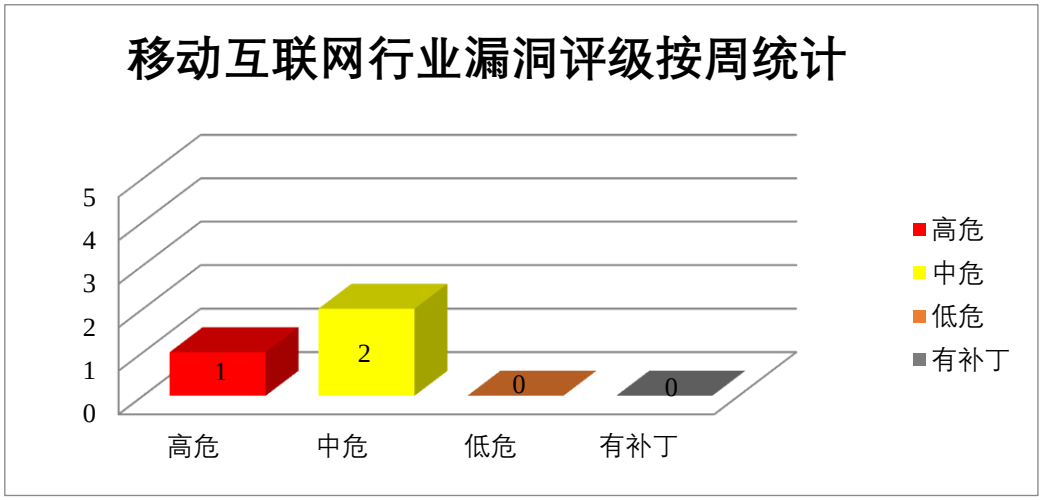


图 4 移动互联网行业漏洞统计

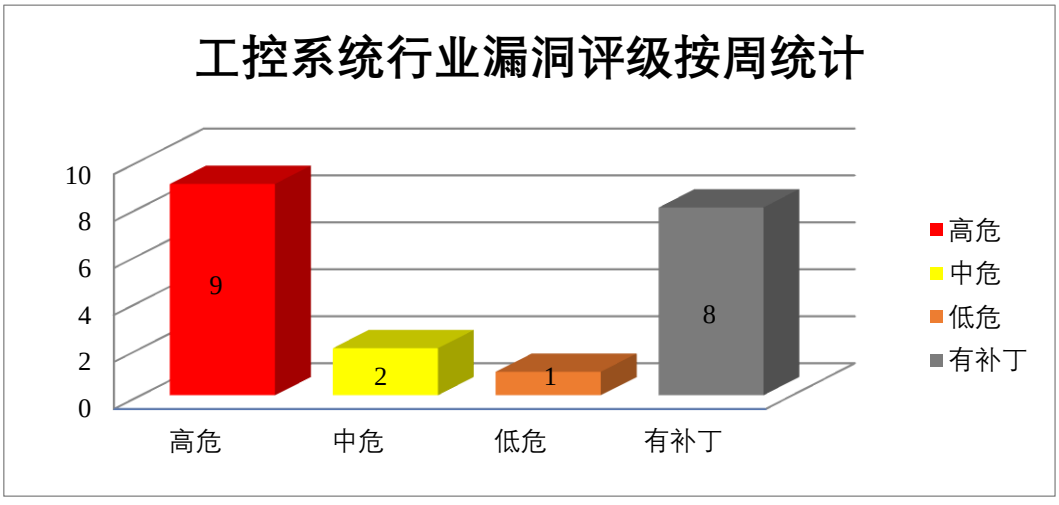


图 5 工控系统行业漏洞统计

## 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 Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe InCopy 是一款用于创作的文本编辑软件。Adobe Substance 3D Stager 是一个虚拟 3D 工作室。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Framemaker 代码问题漏洞（CNVD-2024-40917、CNVD-2024-40916）、Adobe Framemaker 数字错误漏洞、Adobe Framemaker 缓冲区溢出漏洞（CNVD-2024-40921）、Adobe InCopy 代码问题漏洞（CNVD-2024-40920）、Adobe Substance 3D Stager 代码执行漏洞（CNVD-2024-40924、CNVD-2024-40923）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2024-40922）。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-2024-40917
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40916
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40915
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40921
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40920
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40924
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40923
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40922

### 2、 Microsoft 产品安全漏洞

Microsoft Dynamics 365 是美国微软（Microsoft）公司的一套适用于跨国企业的 ERP 业务解决方案。该产品包括财务管理、生产管理和商业智能管理等。Microsoft Dynamics 365 Business Central 是一款全面的业务管理解决方案，可帮助中小型公司在单个易于使用的应用程序中连接其财务、销售、服务和运营团队。Microsoft Windows Hyper-V 是一款可提供硬件虚拟化的工具。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基于 cookie 的身份验证凭据，通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-40534）、Microsoft Dynamics 365 Business Central 权限提升漏洞（CNVD-2024-40535、CNVD-2024-40536）、Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-40537、CNVD-2024-40538）、Microsoft Windows Hyper-V 拒绝服

务漏洞（CNVD-2024-40539、CNVD-2024-40542）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2024-40540）。其中，除“Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-40534）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2024-40540）”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-2024-40534
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40535
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40536
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40537
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40538
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40539
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40540
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40542

### 3、Trend Micro 产品安全漏洞

Trend Micro VPN Proxy One Pro 是美国趋势科技（Trend Micro）公司的一种最佳虚拟专用网络服务。Trend Micro Apex One 是一款终端防护软件。Trend Micro Deep Security 是一种服务器深度安全防护系统客户端。Trend Micro InterScan Web Security Virtual Appliance（IWSVA）是一款针对基于 Web 方式的威胁为企业网络提供动态的、集成式的安全保护的 Web 安全网关。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用户基于 cookie 的身份验证凭据，提升权限，并在系统上下文中执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Trend Micro VPN Proxy One Pro 拒绝服务漏洞、Trend Micro Apex One 访问控制错误漏洞（CNVD-2024-40819）、Trend Micro Apex One 权限提升漏洞（CNVD-2024-40818、CNVD-2024-40826、CNVD-2024-40825）、Trend Micro Apex One 拒绝服务漏洞、Trend Micro Deep Security 权限提升漏洞、Trend Micro InterScan Web Security Virtual Appliance 跨站脚本漏洞（CNVD-2024-40821）。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-2024-40820
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40819
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40818
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40824
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40822
https://www.cnvd.org.cn/flaw/show/CNVD-2024-40821

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40826

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40825

### 4、Foxit 产品安全漏洞

Foxit PDF Reader 是一款 PDF 文档阅读器和打印器，拥有快捷的启动速度和丰富的功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 权限提升漏洞、Foxit PDF Reader 代码执行漏洞（CNVD-2024-40813、CNVD-2024-40812、CNVD-2024-40811、CNVD-2024-40816、CNVD-2024-40815）、Foxit PDF Reader 资源管理错误漏洞（CNVD-2024-40814）、Foxit PDF Reader 释放后重用漏洞（CNVD-2024-40817）。其中，除“Foxit PDF Reader 代码执行漏洞（CNVD-2024-40811）”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-2024-40810

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40813

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40812

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40811

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40816

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40815

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40814

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40817

### 5、D-Link DCS-960L 缓冲区溢出漏洞

D-Link DCS-960L 是中国友讯（D-Link）公司的一款网络摄像头产品。本周，D-Link DCS-960L 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码。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-2024-41036

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-2024-40543 | PDF-XChange Editor XPS 文件解析越界读远程代码执行漏洞 | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.pdf-xchange.com/index.php/support/security-bulletins.html |
| CNVD-2024-40750 | Mozilla Firefox 释放后重用漏洞（CNVD-2024-40750） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新： |

| | | | |
|---|---|---|---|
| | | | https://www.mozilla.org/security/advisories/mfsa2024-51/ |
| CNVD-2024-40774 | PDF-XChange Editor XPS 文件解析越界读远程代码执行漏洞（CNVD-2024-40774） | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.pdf-xchange.com/index.php/support/security-bulletins.html |
| CNVD-2024-40776 | PDF-XChange Editor XPS 文件解析越界读远程代码执行漏洞（CNVD-2024-40776） | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.pdf-xchange.com/index.php/support/security-bulletins.html |
| CNVD-2024-40828 | Delta Electronics CNCSoft-G2 未初始化变量漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft-g2&sort_expr=cdate&sort_dir=DESC |
| CNVD-2024-40831 | Delta Electronics CNCSoft-G2 缓冲区溢出漏洞（CNVD-2024-40831） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft-g2&sort_expr=cdate&sort_dir=DESC |
| CNVD-2024-40830 | Delta Electronics CNCSoft-G2 越界写漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft-g2&sort_expr=cdate&sort_dir=DESC |
| CNVD-2024-40833 | Rockwell Automation 5015-AENFTXT 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://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1680.html |
| CNVD-2024-40834 | Rockwell Automation Pavilion8 路径遍历漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1695.html |
| CNVD-2024-40886 | Oracle WebLogic Server 远程代码执行漏洞（CNVD-2024-40886） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.oracle.com/security-alerts/cpuoct2024.html |

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

此外，Microsoft、Trend Micro、Foxit 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取用户基于 cookie 的身份验证凭据，提升权限，并在系统上下文中执行任意代码，导致拒绝服务等。另外，D-Link DCS-960L 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码。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、Tenda G3 缓冲区溢出漏洞（CNVD-2024-40839）

**验证描述**

Tenda G3 是中国腾达（Tenda）公司的一款 Qos Vpn 路由器。

Tenda G3 15.11.0.20 版本存在缓冲区溢出漏洞，该漏洞源于/goform/setDebugCfg 文件中的 formSetDebugCfg 功能的 enable/level/module 参数未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致应用程序崩溃。

**验证信息**

POC 链接：https://github.com/abcdefg-png/AHU-IoT-vulnerable/blob/main/Tenda/G3V3.0/formSetDebugCfg.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-40839

**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. 新的 macOS 漏洞允许攻击者绕过安全控制

微软威胁情报发现，macOS 出现了一个名为“HM Surf”的新漏洞，能允许攻击者绕过操作系统的透明、同意和控制（TCC）技术，在未经授权的情况下访问用户受保护的数据。

参考链接：https://cybersecuritynews.com/macos-vulnerability-bypass-security-controls/

### 2. Microsoft 在 Windows Server 中弃用 PPTP 和 L2TP VPN 协议

Microsoft 已在未来版本的 Windows Server 中正式弃用点对点隧道协议(PPTP)和第 2 层隧道协议(L2TP)，并建议管理员切换到提供更高安全性的不同协议。

参考链接：https://www.4hou.com/posts/jBnz

## 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