# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2025 年 01 月 06 日-2025 年 01 月 12 日** **2025 年第 2 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 260 个，其中高危漏洞 131 个、中危漏洞 113 个、低危漏洞 16 个。漏洞平均分值为 6.50。本周收录的漏洞中，涉及 0day 漏洞 188 个（占 72%），其中互联网上出现“TOTOLINK AC1200 T8 UploadCustomModule 函数缓冲区溢出漏洞、TOTOLINK AC1200 T8 setWiFiAclRules 函数缓冲区溢出漏洞”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漏洞总数 6039 个，与上周（22622 个）环比减少 73%。

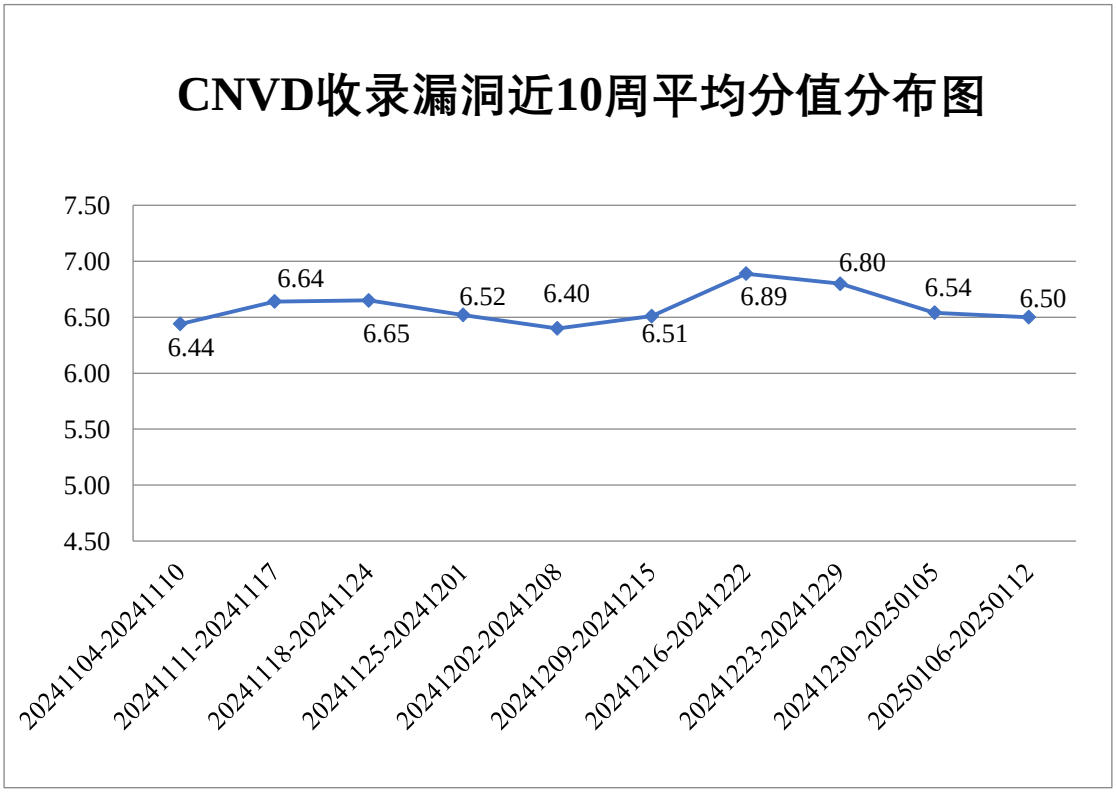


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 1 起，向基础电信企业通报漏洞事件 0 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 557 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 27 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 18 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：

竹门日智能科技（上海）有限公司、珠海金山办公软件有限公司、中卫信软件股份有限公司、中电科金仓（北京）科技股份有限公司、智互联（深圳）科技有限公司、浙江中控技术股份有限公司、浙江宇视科技有限公司、用友网络科技股份有限公司、新都（青岛）电子有限公司、无锡信捷电气股份有限公司、万洲电气股份有限公司、苏州欧信达信息科技有限公司、深圳致软信息技术有限公司、深圳市中科网威科技有限公司、深圳市亿玛信诺科技有限公司、深圳市思迅软件股份有限公司、深圳市世纪伟图科技开发有限公司、深圳市锐明技术股份有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市富士智能科技有限公司、深圳市顶讯网络科技有限公司、深圳勤杰软件有限公司、深圳警翼智能科技股份有限公司、深圳邦健生物医疗设备股份有限公司、深圳奥哲网络科技有限公司、上海卓卓网络科技有限公司、上海云翌通信科技有限公司、上海上讯信息技术股份有限公司、上海安艺网络科技有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山西牛之云网络科技有限公司、山东仁科测控技术有限公司、厦门微信软件有限公司、厦门天锐科技股份有限公司、三星（中国）投资有限公司、麒麟软件有限公司、龙采科技集团有限责任公司、力合科技（湖南）股份有限公司、廊坊市极致网络科技有限公司、蓝卓数字科技有限公司、蓝信移动（北京）科技有限公司、可豪软件信息技术南京有限公司、济南卓源软件有限公司、济南驰骋信息技术有限公司、吉翁电子（深圳）有限公司、湖南众合百易信息技术有限公司、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、瀚高基础软件股份有限公司、广州图创计算机软件开发有限公司、广州市天翎网络科技有限公司、广州酷狗计算机科技有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东数夫软件有限公司、高新兴科技集团股份有限公司、佛山市杜特软件科技有限公司、泛微网络科技股份有限公司、东莞市同享软件科技有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、比亚迪股份有限公司、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京亚控科技发展有限公司、北京万里开源软件有限公司、北京数字认证股份有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京趋势威尔网络技术有限公司、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、北京百度网讯科技有限公司、安科瑞电气股份有限公司、艾默生网络能源有限公司和 Lexmark。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、新华三技术有限公司、安天科技集团股份有限公司、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。苏州棱镜七彩信息科技有限公司、江苏云天网络安全技术有限公司、北京翰慧投资咨询有限公司、北京山石网科信息技术有限公司、北京纽盾网安信息技术有限公司、成都卫士通信息安全技术有限公司、北京天下信安技术有限公司、江苏正信信息安全测试有限公司、淮安易云科技有限公司、中资网络信息安全科技有限公司、超聚变数字技术有限公司、贵州多彩网安科技有限公司、成都久信信息技术股份有限公司、北京安帝科技有限公司、杭州默安科技有限公司、北京时代新威信息技术有限公司、宁夏凯信特信息科技有限公司、联通数字科技有限公司、北京大学长沙计算与数字经济研究院、深圳市博通智能技术有限公司、星云博创科技有限公司、江苏君立华域信息安全技术股份有限公司、上海谋乐网络科技有限公司、浙江大学控制科学与工程学院、北京网御星云信息技术有限公司、河南东方云盾信息技术有限公司、浙江微特电子信息有限公司、江苏保旺达软件技术有限公司、江苏力可信网络科技有限公司及其他个人白帽子向 CNVD 提交了 6039 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 4666 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） | 3282 | 3282 |
| 三六零数字安全科技集团有限公司 | 1207 | 1207 |
| 北京启明星辰信息安全技术有限公司 | 609 | 19 |
| 新华三技术有限公司 | 426 | 0 |
| 安天科技集团股份有限公司 | 393 | 0 |
| 北京神州绿盟科技有限公司 | 365 | 0 |
| 阿里云计算有限公司 | 287 | 3 |
| 上海交大 | 177 | 177 |
| 深信服科技股份有限公司 | 177 | 0 |

| | | |
|---|---|---|
| 杭州安恒信息技术股份有限公司 | 129 | 27 |
| 北京知道创宇信息技术有限公司 | 124 | 0 |
| 北京天融信网络安全技术有限公司 | 58 | 8 |
| 中国电信集团系统集成有限责任公司 | 29 | 0 |
| 北京安信天行科技有限公司 | 27 | 27 |
| 北京长亭科技有限公司 | 23 | 13 |
| 杭州迪普科技股份有限公司 | 21 | 0 |
| 南京众智维信息科技有限公司 | 6 | 6 |
| 北京智游网安科技有限公司 | 5 | 5 |
| 华为技术有限公司 | 5 | 5 |
| 北京升鑫网络科技有限公司（青藤云安全） | 2 | 2 |
| 奇安信网神（补天平台） | 1 | 1 |
| 西安四叶草信息技术有限公司 | 1 | 1 |
| 苏州棱镜七彩信息科技有限公司 | 19 | 19 |
| 江苏云天网络安全技术有限公司 | 18 | 18 |
| 北京翰慧投资咨询有限公司 | 11 | 11 |
| 北京山石网科信息技术有限公司 | 11 | 11 |
| 北京纽盾网安信息技术有限公司 | 9 | 9 |

| | | |
|---|---|---|
| 成都卫士通信息安全技术有限公司 | 8 | 8 |
| 北京天下信安技术有限公司 | 7 | 7 |
| 江苏正信信息安全测试有限公司 | 3 | 3 |
| 淮安易云科技有限公司 | 3 | 3 |
| 中资网络信息安全科技有限公司 | 2 | 2 |
| 超聚变数字技术有限公司 | 2 | 2 |
| 贵州多彩网安科技有限公司 | 2 | 2 |
| 成都久信信息技术股份有限公司 | 2 | 2 |
| 北京安帝科技有限公司 | 2 | 2 |
| 杭州默安科技有限公司 | 1 | 1 |
| 北京时代新威信息技术有限公司 | 1 | 1 |
| 宁夏凯信特信息科技有限公司 | 1 | 1 |
| 联通数字科技有限公司 | 1 | 1 |
| 北京大学长沙计算与数字经济研究院 | 1 | 1 |
| 深圳市博通智能技术有限公司 | 1 | 1 |
| 星云博创科技有限公司 | 1 | 1 |
| 江苏君立华域信息安全技术股份有限公司 | 1 | 1 |
| 上海谋乐网络科技有 | 1 | 1 |

| | | |
|---|---|---|
| 限公司 | | |
| 浙江大学控制科学与工程学院 | 1 | 1 |
| 北京网御星云信息技术有限公司 | 1 | 1 |
| 河南东方云盾信息技术有限公司 | 1 | 1 |
| 浙江微特电子信息有限公司 | 1 | 1 |
| 江苏保旺达软件技术有限公司 | 1 | 1 |
| 江苏力可信网络科技有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 5 | 5 |
| CNCERT 河南分中心 | 4 | 4 |
| CNCERT 河北分中心 | 2 | 2 |
| 个人 | 1131 | 1131 |
| 报送总计 | 8610 | 6039 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 260 个漏洞。WEB 应用 132 个，应用程序 64 个，网络设备（交换机、路由器等网络端设备）37 个，操作系统 11 个，智能设备（物联网终端设备）9 个，安全产品 5 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 | 132 |
| 应用程序 | 64 |
| 网络设备（交换机、路由器等网络端设备） | 37 |
| 操作系统 | 11 |
| 智能设备（物联网终端设备） | 9 |
| 安全产品 | 5 |
| 数据库 | 2 |

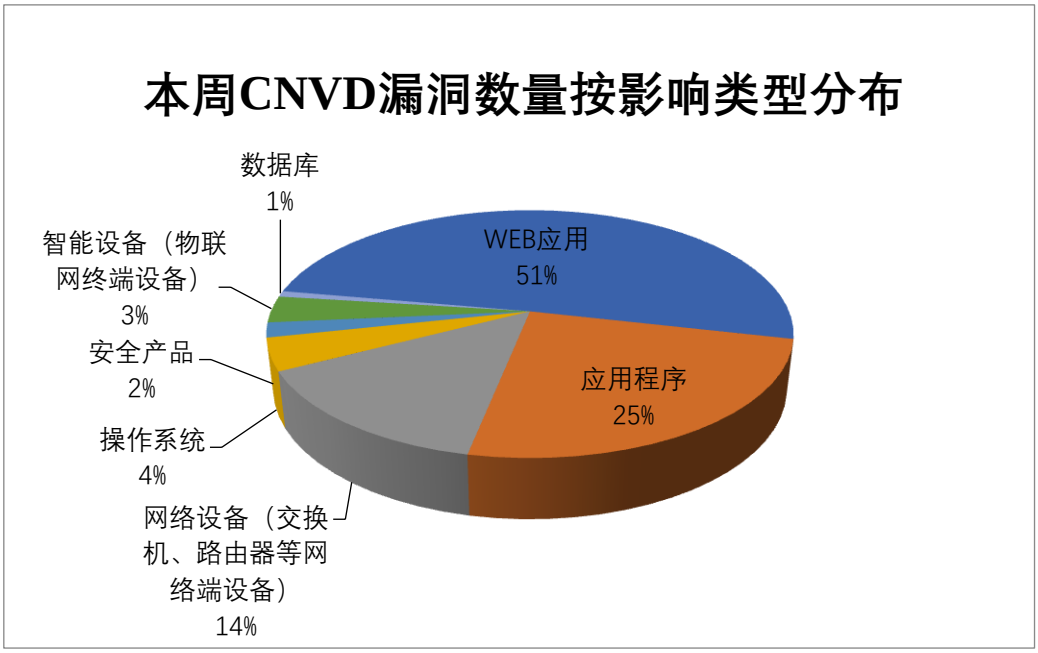


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Fortinet、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 | Adobe | 14 | 5% |
| 2 | Fortinet | 10 | 4% |
| 3 | Mozilla | 10 | 4% |
| 4 | IBM | 9 | 3% |
| 5 | 用友网络科技股份有限公司 | 8 | 3% |
| 6 | 青岛海信网络科技股份有限公司 | 5 | 2% |
| 7 | 畅捷通信息技术股份有限公司 | 5 | 2% |
| 8 | Huawei | 5 | 2% |
| 9 | D-Link | 5 | 2% |
| 10 | 其他 | 189 | 73% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞，9 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Google Android 信息泄露漏洞（CNVD-2025-00875）、Google Android 拒绝服务漏洞（CNVD-2025-00876）”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/

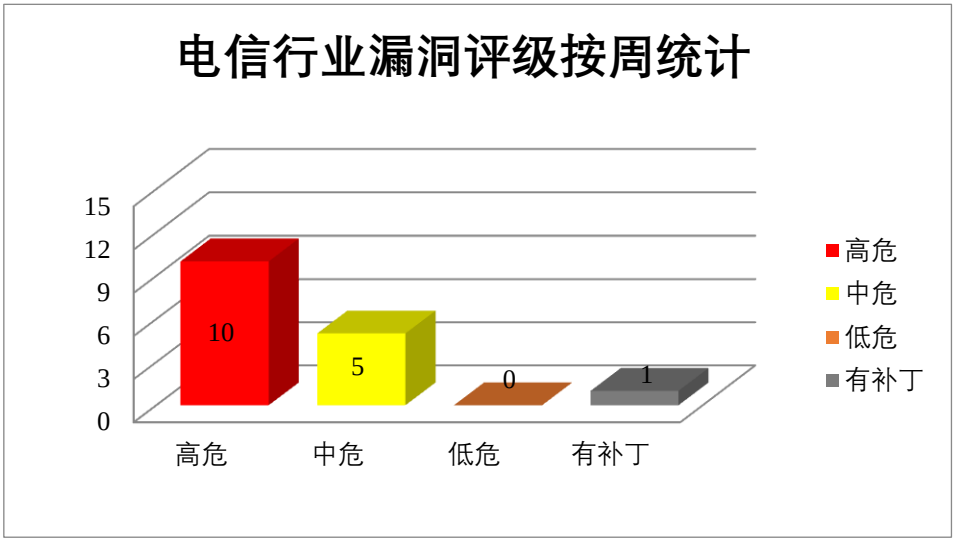


图 3 电信行业漏洞统计

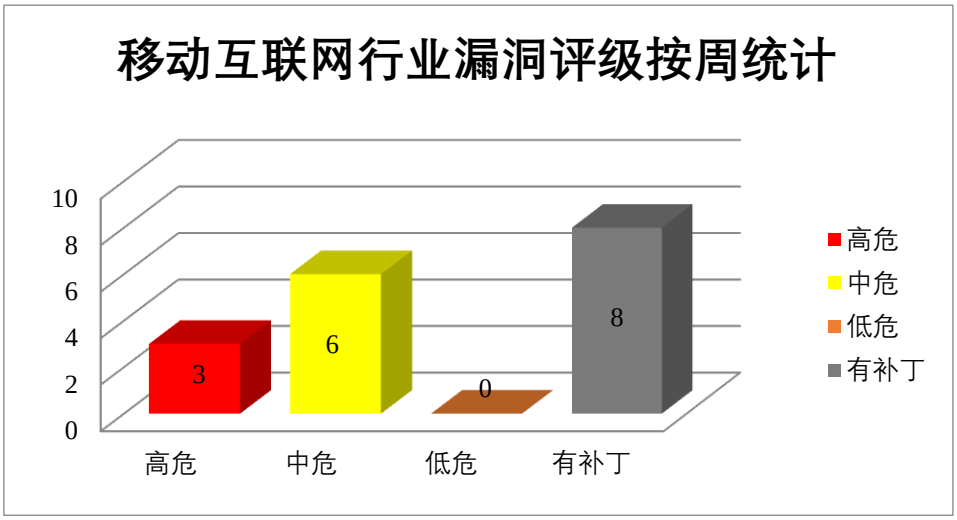


图 4 移动互联网行业漏洞统计

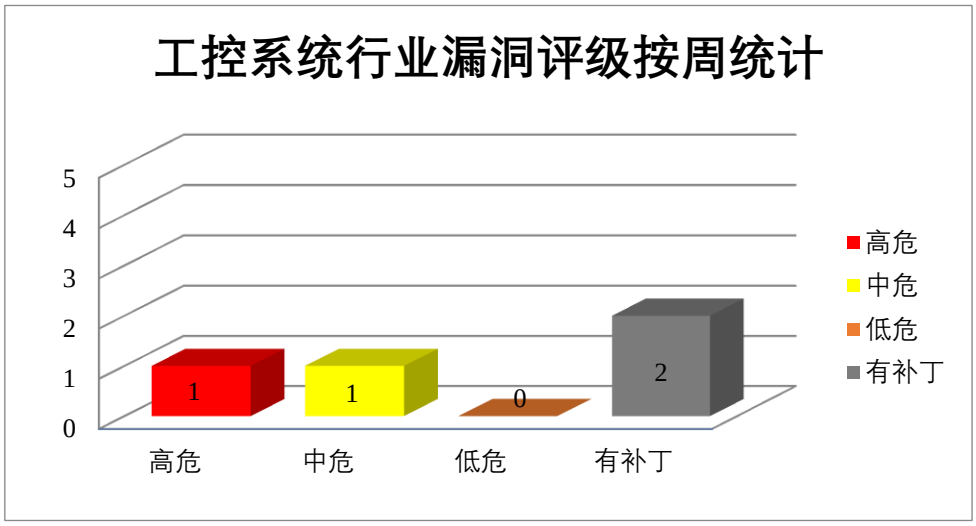


图 5 工控系统行业漏洞统计

## 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、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏览器）的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。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，在易受攻击的系统上执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Thunderbird 未授权访问漏洞、Mozilla Firefox 和 Thunderbird 信息泄露漏洞（CNVD-2025-00859）、多款 Mozilla 产品代码执行漏洞（CNVD-2025-00862、CNVD-2025-00866）、Mozilla Firefox 和 Thunderbird 拒绝服务漏洞（CNVD-2025-00863、CNVD-2025-00864）、Mozilla Firefox 和 Thunderbird 代码执行漏洞（CNVD-2025-00865）、Mozilla Thunderbird 信息泄露漏洞（CNVD-2025-00867）。其中，除“Mozilla Thunderbird 信息泄露漏洞（CNVD-2025-00867）”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-2025-00858

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00859

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00862

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00863

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00864

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00865

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00866

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00867

## 2、Adobe 产品安全漏洞

Adobe Substance 3D Modeler 是美国奥多比（Adobe）公司的一款 3D 建模和雕刻软件。Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。Adobe Substance 3D Sampler 是美国奥多比（Adobe）公司的一款摄影测量软件。用于将照片捕捉和扫描图像转换为 3D 纹理和材质资产。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Modeler 越界写入漏洞（CNVD-2025-00377、CNVD-2025-00378）、Adobe Substance 3D Modeler 堆缓冲区溢出漏洞（CNVD-2025-00382）、Adobe Substance 3D Modeler 越界写入漏洞、Adobe Substance 3D Painter 堆缓冲区溢出漏洞（CNVD-2025-00384）、Adobe Substance 3D Painter 越界写入漏洞（CNVD-2025-00383）、Adobe Substance 3D Sampler 越界写入漏洞（CNVD-2025-00386）、Adobe Substance 3D Sampler 堆缓冲区溢出漏洞（CNVD-2025-00385）。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-2025-00377

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00378

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00382

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00381

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00384

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00383

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00386

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00385

## 3、IBM 产品安全漏洞

IBM Cognos Analytics 是美国国际商业机器（IBM）公司的一套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。IBM Storage Defender 是美国国际商业机器（IBM）公司的一种提供端到端数据弹性的解决方案。IBM MQ 是美国国际商业机器（IBM）公司的一款消息传递中间件产品。该产品主要为面向服务的体系结构（SOA）提供可靠的、经过验证的消息传递主干网。IBM Robotic Process Automation 是美国国际商业机器（IBM）公司的一种机器人流程自动化产品。可帮助您以传统 RPA 的轻松和速度大规模自动化更多业务和 IT 流程。IBM App Connect Enterprise 是 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。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，执行恶意命令，

导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Cognos Analytics 跨站脚本漏洞（CNVD-2025-00306）、IBM Storage Defender 明文传输漏洞、IBM MQ 拒绝服务漏洞（CNVD-2025-00308）、IBM Cognos Analytics 输入验证错误漏洞（CNVD-2025-00307）、IBM Robotic Process Automation 信息泄露漏洞（CNVD-2025-00312）、IBM MQ Appliance 缓冲区溢出漏洞（CNVD-2025-00311）、IBM Storage Defender 信任管理问题漏洞、IBM App Connect Enterprise 拒绝服务漏洞（CNVD-2025-00874）。其中，“IBM Robotic Process Automation 信息泄露漏洞（CNVD-2025-00312）”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-2025-00306
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00309
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00308
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00307
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00312
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00311
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00310
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00874

### 4、Fortinet 产品安全漏洞

Fortinet FortiEDR 是美国飞塔（Fortinet）公司的一个从头开始构建的端点安全解决方案。Fortinet FortiClientEMS 是美国飞塔（Fortinet）公司的 Fortinet 提供的端点管理解决方案的一部分，旨在帮助组织有效地管理其网络中的终端设备，并提供端点安全性的监控和控制。Fortinet FortiManager 是美国飞塔（Fortinet）公司的一套集中化网络安全管理平台。该平台支持集中管理任意数量的 Fortinet 设备，并能够将设备分组到不同的管理域（ADOM）进一步简化多设备安全部署与管理。Fortinet FortiAIOps 是美国飞塔（Fortinet）公司的一款结合人工智能与机器学习(AI/ML) 的 Fortinet 网络配套解决方案。Fortinet FortiSOAR 是美国飞塔（Fortinet）公司的一种安全编排、自动化和响应(SOAR) 解决方案。Fortinet FortiWLM 是美国飞塔（Fortinet）公司的一个无线管理器。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，导致任意命令执行等。

CNVD 收录的相关漏洞包括：Fortinet FortiEDR 访问控制错误漏洞（CNVD-2025-00410）、Fortinet FortiClientEMS 命令注入漏洞、Fortinet FortiManager 访问控制错误漏洞（CNVD-2025-00408）、Fortinet FortiAIOps 日志信息泄露漏洞、Fortinet FortiAIOps 跨站请求伪造漏洞、Fortinet FortiAIOps 代码问题漏洞、Fortinet FortiSOAR 跨站脚本漏洞（CNVD-2025-00411）、Fortinet FortiWLM 路径遍历漏洞（CNVD-2025-00417）。其中，除“Fortinet FortiEDR 访问控制错误漏洞（CNVD-2025-00410）、Fortinet Forti

AIOps 日志信息泄露漏洞”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-2025-00410
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00409
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00408
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00414
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00413
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00412
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00411
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00417

### 5、D-Link DAP-1520 拒绝服务漏洞

D-Link DAP-1520 是中国友讯（D-Link）公司的一款无线接入点产品。本周，D-Link DAP-1520 被披露存在拒绝服务漏洞，攻击者可利用该漏洞导致拒绝服务。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-2025-00879

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-2025-00381 | Adobe Substance 3D Modeler 越界写入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html |
| CNVD-2025-00413 | Fortinet FortiAIOps 跨站请求伪造漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.fortinet.com/psirt/FG-IR-24-070 |
| CNVD-2025-00858 | Mozilla Firefox 和 Thunderbird 未经授权访问漏洞 | 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/mfsa2024-63/ https://www.mozilla.org/security/advisories/mfsa2024-67/ |
| CNVD-2025-00387 | Adobe Substance 3D Sampler 堆缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/prod |

| | | | |
|---|---|---|---|
| | | | ucts/substance3d-sampler/apsb24-100.html |
| CNVD-2025-00869 | Huawei HarmonyOS 图像解码模块读/写漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2024/12/ |
| CNVD-2025-00875 | Google Android 信息泄露漏洞（CNVD-2025-00875） | 高 | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://source.android.com/docs/security/bulletin/pixel/2018-05-01 |
| CNVD-2025-00881 | Rockwell Automation Arena Simulation DOE 文件内存错误引用代码执行漏洞 | 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.rockwellautomation.com/ |
| CNVD-2025-00376 | Adobe Substance 3D Modeler 越界写入漏洞（CNVD-2025-00376） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html |
| CNVD-2025-00417 | Fortinet FortiWLM 路径遍历漏洞（CNVD-2025-00417） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-23-143 |
| CNVD-2025-00383 | Adobe Substance 3D Painter 越界写入漏洞（CNVD-2025-00383） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/substance3d_painter/apsb24-105.html |

小结：本周，Mozilla 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，在易受攻击的系统上执行任意代码或造成拒绝服务等。此外，Adobe、IBM、Fortinet 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，在当前用户的上下文中执行任意代码，导致拒绝服务等。另外，D-Link DAP-1520 被披露存在拒绝服务漏洞，攻击者可利用该漏洞导致拒绝服务。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、TOTOLINK AC1200 T8 UploadCustomModule 函数缓冲区溢出漏洞

**验证描述**

TOTOLINK AC1200 T8 是中国吉翁电子（TOTOLINK）公司的一款双频全千兆路

由器。

TOTOLINK AC1200 T8 UploadCustomModule 函数存在缓冲区溢出漏洞，该漏洞源于 UploadCustomModule 函数的 File 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拒绝服务。

**验证信息**

POC 链接：https://github.com/TTTJJJWWW/AHU-IoT-vulnerable/blob/main/TOTOLINK/AC1200T8/UploadCustomModule.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2025-00877

**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. Palo Alto Networks Expedition Tool 漏洞暴露了防火墙凭证

Palo Alto Networks 的 Expedition 迁移工具中发现了多个漏洞，这些漏洞可能会暴露敏感的防火墙凭据，包括用户名、明文密码、设备配置和 API 密钥。

参考链接：https://cybersecuritynews.com/palo-alto-networks-expedition-tool-vulnerability/#google_vignette

### 2. Dell Update Package Framework 漏洞允许攻击者提升权限

戴尔的更新包 （DUP） 框架中发现一个安全漏洞，该漏洞可能会使系统面临权限提升和拒绝服务攻击。

参考链接：https://cybersecuritynews.com/dell-update-vulnerability/

**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