# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2025 年 05 月 12 日-2025 年 05 月 18 日　　2025 年第 18 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 363 个，其中高危漏洞 181 个、中危漏洞 166 个、低危漏洞 16 个。漏洞平均分值为 6.65。本周收录的漏洞中，涉及 0day 漏洞 273 个（占 75%），其中互联网上出现“TOTOLINK A810R 缓冲区溢出漏洞、TOTOLINK A800R v14 参数缓冲区溢出漏洞”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 11049 个，与上周（10728 个）环比增加 3%。

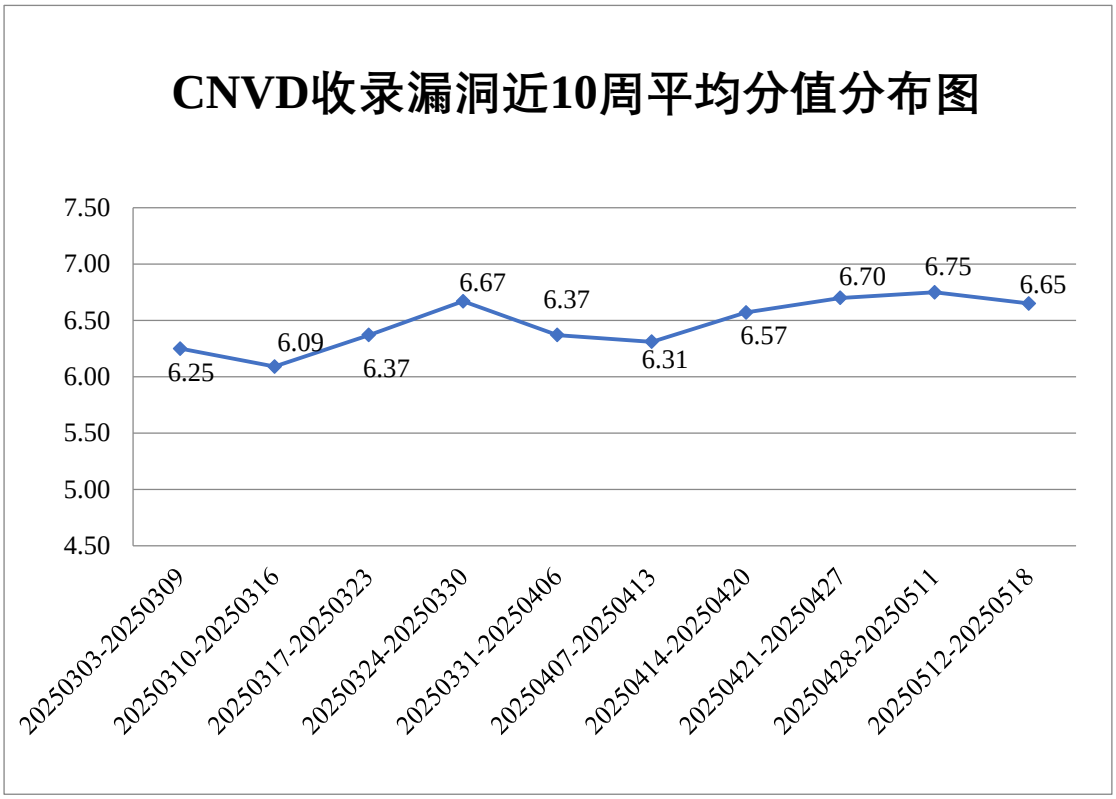


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 3 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 623 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 24 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：

紫光股份有限公司、重庆中联信息产业有限责任公司、重庆金商软件有限公司、中版行知（广州）数字传媒有限公司、智者四海（北京）技术有限公司、智慧互通科技股份有限公司、智互联（深圳）科技有限公司、郑州三晖电气股份有限公司、浙江和达科技股份有限公司、掌如科技（成都）有限公司、云和恩墨（北京）信息技术有限公司、昱能科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、依米康科技集团股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、武汉盛帆电子股份有限公司、网件（北京）网络技术有限公司、万洲电气股份有限公司、统信软件技术有限公司、同望科技股份有限公司、同方股份有限公司、天闻数媒科技（北京）有限公司、天津环球磁卡集团有限公司、腾讯安全应急响应中心、台达电子企业管理（上海）有限公司、苏州语灵人工智能科技有限公司、苏州新建元控股集团有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、神州云科（北京）科技有限公司、深圳市中电电力技术股份有限公司、深圳市雨田软件技术有限公司、深圳市蓝凌软件股份有限公司、深圳市科脉技术股份有限公司、深圳市锦辰科技有限公司、深圳市嘉荣华科技有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳建广数字科技有限公司、深圳国威电子有限公司、深圳达实智能股份有限公司、深信服科技股份有限公司、上海卓卓网络科技有限公司、上海卓佑计算机技术有限公司、上海真兰仪表科技股份有限公司、上海夏普电器有限公司、上海物创信息科技有限公司、上海铜哨科技有限公司、上海上讯信息技术股份有限公司、上海三高计算机中心股份有限公司、上海茸易科技有限公司、上海企望信息科技有限公司、上海肯特仪表股份有限公司、上海居亦科技发展有限公司、上海金慧软件有限公司、上海建业信息科技股份有限公司、上海寰创通信科技股份有限公司、上海德米萨信息科技有限公司、上海百胜软件股份有限公司、善理通益信息科技（深圳）有限公司、山东潍微科技股份有限公司、山东泰物信息技术有限公司、山东胜软科技股份有限公司、山东力创科技有限公司、山东金钟科技集团股份有限公司、厦门一指通智能科技有限公司、厦门四信通信科技有限公司、厦门闪酷科技开发有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、瑞纳智能设备股份有限公司、青岛三利中德美水设备有限公司、青岛海信网络科技股份有限公司、罗克

韦尔自动化（中国）有限公司、联奕科技股份有限公司、联想（北京）有限公司、理光（中国）投资有限公司、浪潮电子信息产业股份有限公司、朗坤智慧科技股份有限公司、柯尼卡美能达集团、京瓷（中国）商贸有限公司上海分公司、江西铭软科技有限公司、江苏南大先腾信息产业有限公司、江苏金智教育信息股份有限公司、佳能（中国）有限公司、济南有人物联网技术有限公司、济南拓兴电子科技有限公司、北京火绒网络科技有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南众合百易信息技术有限公司、湖南匠领科技有限公司、鸿合科技股份有限公司、河南小皮安全技术有限公司、河北先河环保科技股份有限公司、杭州三汇信息工程有限公司、杭州灰牛科技有限公司、汉王科技股份有限公司、国电南京自动化股份有限公司、贵州先知科技有限公司、广州通则康威科技股份有限公司、广州市保伦电子有限公司、广州三晶电气股份有限公司、广联达科技股份有限公司、广东中设智控科技股份有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、福建新大陆通信科技股份有限公司、福建博思软件股份有限公司、东芝（中国）有限公司、大连亿坊电子商务有限公司、成都臻识科技发展有限公司、成都虚谷伟业科技有限公司、成都博友科技开发有限公司、畅捷通信息技术股份有限公司、北京子雯互联科技有限公司、北京中控智慧科技发展有限公司、北京智信资管云教育科技有限公司、北京真视通科技股份有限公司、北京用友政务软件股份有限公司、北京亿玛在线科技股份有限公司、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、北京网动网络科技股份有限公司、北京同方卫康科技有限公司、北京世纪百易网络有限公司、北京神州视翰科技有限公司、北京趋势威尔网络技术有限公司、北京灵州网络技术有限公司、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、北京华普亿方科技集团股份有限公司、北京华璨电子有限公司、北京宏景世纪软件股份有限公司、北京瀚维特科技有限公司、北京国遥新天地信息技术股份有限公司、北京东华原医疗设备有限责任公司、北京超图软件股份有限公司、北京百度网讯科技有限公司、北京奥博威斯科技有限公司、百度安全应急响应中心、安科瑞电气股份有限公司和爱普生（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，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、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。北京天下信安技术有限公司、北京时代新威信息技术有限公司、北京山石网科信息技术有限公司、中资网络信息安全科技有限公司、南京经纬信安科技有限公司、苏州棱镜七彩信息科技有限公司、工业和信息化部电子第五研究所、济南三泽信息安全测评有限公司、润成安全技术有限公司、中国电信股份有限公司研究院、山东新潮信息技术有限公司、南方电网科学研究院有限责

任公司、成都久信信息技术股份有限公司、畅捷通信息技术股份有限公司、交通运输部南海航海保障中心、青海祥润网络科技有限公司、中电福富信息科技有限公司、江苏国保信息系统测评中心有限公司、浙江木链物联网科技有限公司、河南灵创电子科技有限公司、北京神州泰岳软件股份有限公司、北京卓识网安技术股份有限公司、亚信科技（成都）有限公司及其他个人白帽子向 CNVD 提交了 11049 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奇安信网神（补天平台）向 CNVD 共享的白帽子报送 9980 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） | 9546 | 9546 |
| 北京启明星辰信息安全技术有限公司 | 2372 | 1 |
| 新华三技术有限公司 | 1305 | 0 |
| 深信服科技股份有限公司 | 1034 | 3 |
| 三六零数字安全科技集团有限公司 | 296 | 296 |
| 杭州安恒信息技术股份有限公司 | 277 | 0 |
| 北京神州绿盟科技有限公司 | 141 | 0 |
| 奇安信网神（补天平台） | 138 | 138 |
| 阿里云计算有限公司 | 126 | 7 |
| 北京天融信网络安全技术有限公司 | 88 | 18 |
| 安天科技集团股份有限公司 | 35 | 0 |
| 华为技术有限公司 | 16 | 16 |
| 杭州迪普科技股份有限公司 | 10 | 1 |
| 快页信息技术有限公司 | 5 | 5 |
| 中国电信股份有限公司网络安全产品运营 | 4 | 4 |

| | | |
|---|---|---|
| 中心 | | |
| 北京知道创宇信息技术有限公司 | 3 | 3 |
| 西安四叶草信息技术有限公司 | 3 | 3 |
| 恒安嘉新（北京）科技股份公司 | 2 | 0 |
| 北京长亭科技有限公司 | 2 | 2 |
| 南京众智维信息科技有限公司 | 2 | 2 |
| 北京安信天行科技有限公司 | 2 | 2 |
| 北京智游网安科技有限公司 | 1 | 1 |
| 深圳市腾讯计算机系统有限公司（玄武实验室） | 1 | 1 |
| 北京天下信安技术有限公司 | 43 | 43 |
| 亚信科技（成都）有限公司 | 16 | 16 |
| 北京时代新威信息技术有限公司 | 13 | 13 |
| 北京山石网科信息技术有限公司 | 5 | 5 |
| 中资网络信息安全科技有限公司 | 4 | 4 |
| 南京经纬信安科技有限公司 | 3 | 3 |
| 苏州棱镜七彩信息科技有限公司 | 3 | 3 |
| 工业和信息化部电子第五研究所 | 3 | 3 |
| 济南三泽信息安全测 | 2 | 2 |

| | | |
|---|---|---|
| 评有限公司 | | |
| 润成安全技术有限公司 | 2 | 2 |
| 中国电信股份有限公司研究院 | 2 | 2 |
| 山东新潮信息技术有限公司 | 2 | 2 |
| 南方电网科学研究院有限责任公司 | 2 | 2 |
| 成都久信信息技术股份有限公司 | 2 | 2 |
| 畅捷通信息技术股份有限公司 | 1 | 1 |
| 交通运输部南海航海保障中心 | 1 | 1 |
| 青海祥润网络科技有限公司 | 1 | 1 |
| 中电福富信息科技有限公司 | 1 | 1 |
| 江苏国保信息系统测评中心有限公司 | 1 | 1 |
| 浙江木链物联网科技有限公司 | 1 | 1 |
| 河南灵创电子科技有限公司 | 1 | 1 |
| 北京神州泰岳软件股份有限公司 | 1 | 1 |
| 北京卓识网安技术股份有限公司 | 1 | 1 |
| 个人 | 889 | 889 |
| 报送总计 | 16409 | 11049 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 363 个漏洞。网络设备（交换机、路由器等网络端设备）134

个，WEB 应用 122 个，应用程序 63 个，智能设备（物联网终端设备）33 个，操作系统 9 个，安全产品 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 |
|---|---|
| 网络设备（交换机、路由器等网络端设备） | 134 |
| WEB 应用 | 122 |
| 应用程序 | 63 |
| 智能设备（物联网终端设备） | 33 |
| 操作系统 | 9 |
| 安全产品 | 2 |

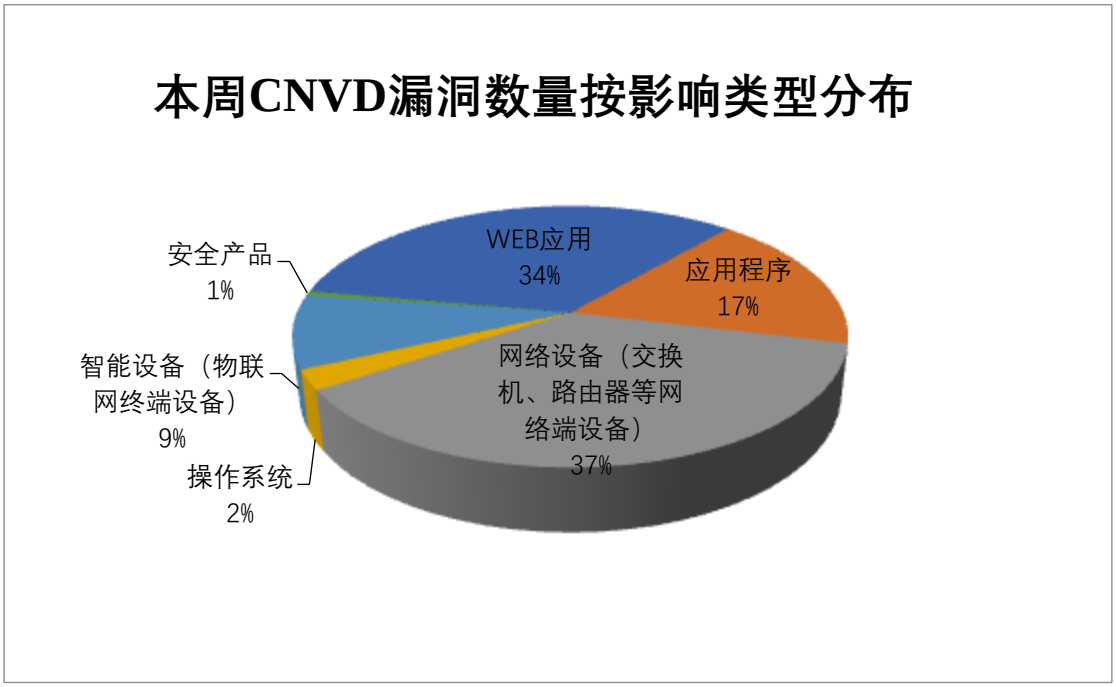


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、TOTOLINK、北京星网锐捷网络技术有限公司等多家厂商的产品，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 | 51 | 14% |
| 2 | TOTOLINK | 20 | 6% |
| 3 | 北京星网锐捷网络技术有限公司 | 14 | 4% |
| 4 | DELL | 10 | 3% |
| 5 | lunary | 10 | 3% |
| 6 | GNU | 10 | 3% |
| 7 | Microsoft | 9 | 2% |

| | | | |
|---|---|---|---|
| 8 | Siemens | 8 | 2% |
| 9 | 畅捷通信息技术股份有限公司 | 7 | 2% |
| 10 | 其他 | 224 | 61% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 79 个电信行业漏洞，6 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“TOTOLINK N150RT /boafrm/formPortFw 文件缓冲区溢出漏洞、Ivanti Endpoint Manager Mobile 代码执行漏洞、Siemens SCALANCE LPE 9403 SFTP 功能路径遍历漏洞”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/

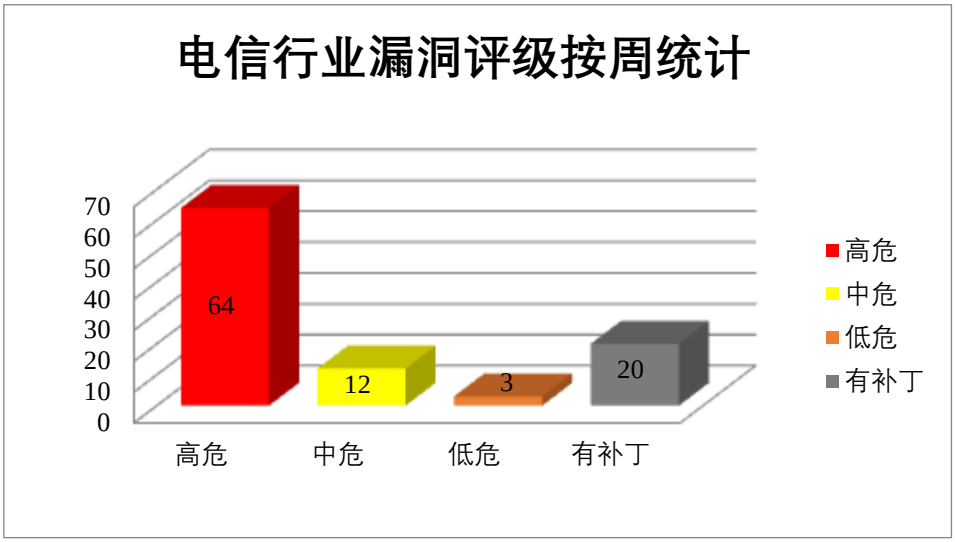


图 3 电信行业漏洞统计

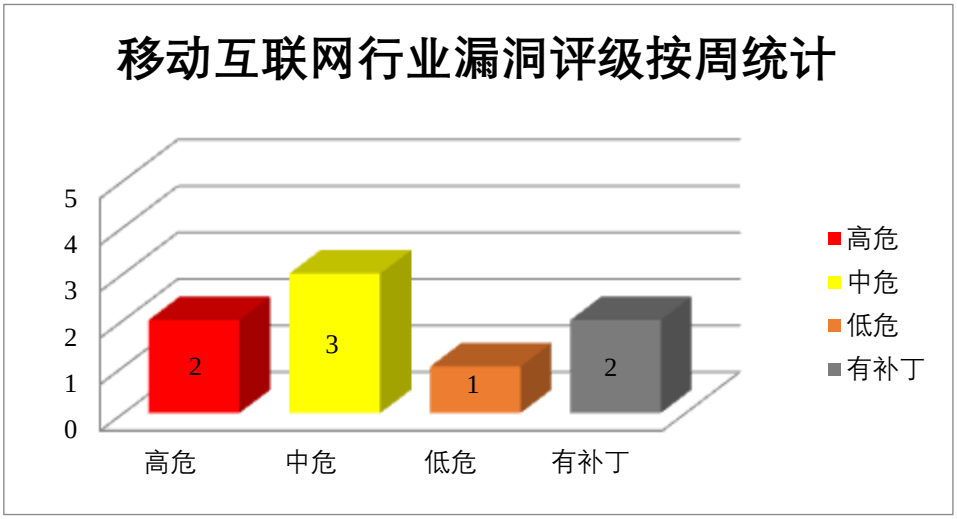


图 4 移动互联网行业漏洞统计

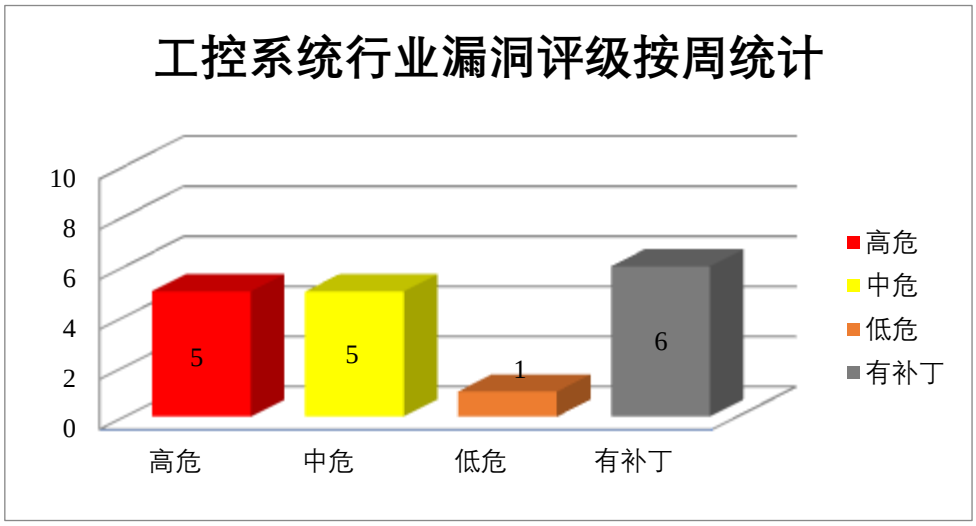


图 5 工控系统行业漏洞统计

## 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、 Siemens 产品安全漏洞

Siemens OpenV2G 是德国西门子（Siemens）公司的一种 V2G 基础设施组件的开源实现。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。该软件通过从多种机械计算机辅助设计（MCAD）格式创建虚拟原型，可简化了工程和制造流程。Siemens Tecnomatix Plant Simulation 是一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。Siemens SCALANCE LPE9403 是德国西门子（Siemens）公司的一款用于工业现场数据处理的本地处理引擎。用于捕获、收集和预处理工业现场数据。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取和写入任意文件，执行任意代码，导致内存破坏。

CNVD 收录的相关漏洞包括：Siemens OpenV2G 缓冲区溢出漏洞、Siemens Teamcenter Visualization 和 Siemens Tecnomatix Plant Simulation 资源管理错误漏洞、Siemens Teamcenter Visualization 和 Siemens Tecnomatix Plant Simulation 缓冲区溢出漏洞（CNVD-2025-09578、CNVD-2025-09959）、Siemens SCALANCE LPE9403 SFTP 功能路径遍历漏洞、Siemens Teamcenter Visualization 缓冲区溢出漏洞（CNVD-2025-09960）、Siemens SCALANCE LPE9403 操作系统命令注入漏洞（CNVD-2025-09961、CNVD-2025-09962）。其中，除“Siemens OpenV2G 缓冲区溢出漏洞”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-2025-09488
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09523
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09578
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09579
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09959
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09960
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09961
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09962

## 2、 Microsoft 产品安全漏洞

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Word 是美国微软（Microsoft）公司的一套 Office 套件中的文字处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Edge (Chromium-based)欺骗漏洞（CNVD-2025-09951）、Microsoft Office 代码执行漏洞（CNVD-2025-09952、CNVD-2025-09955）、Microsoft Excel 代码执行漏洞（CNVD-2025-09953、CNVD-2025-09954）、Microsoft Word 代码执行漏洞（CNVD-2025-09956、CNVD-2025-09957、CNVD-2025-09958）。其中，除“Microsoft Edge (Chromium-based)欺骗漏洞（CNVD-2025-09951）、Microsoft Word 代码执行漏洞（CNVD-2025-09957）”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-2025-09951
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09952
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09953

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09954

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09955

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09956

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09957

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09958

### 3、Dell 产品安全漏洞

Dell PowerProtect Data Manager Reporting 是一款数据保护管理软件。Dell Trusted Device 是美国戴尔（Dell）公司的一款应用程序。Dell RecoverPoint for Virtual Machines 是美国戴尔（Dell）公司的一种简单、高效的操作和灾难恢复解决方案。Dell PowerScale OneFS 是美国戴尔（Dell）公司的一个操作系统。Dell Wyse Management Suite 是美国戴尔（Dell）公司的一个云端与本地管理平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，修改配置，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Dell PowerProtect Data Manager Reporting 权限提升漏洞、Dell Trusted Device 权限提升漏洞、Dell Trusted Device 后置链接漏洞、Dell RecoverPoint for Virtual Machines 命令执行漏洞、Dell PowerScale OneFS 默认密码漏洞、Dell PowerScale OneFS 资源消耗漏洞、Dell PowerScale OneFS 整数溢出漏洞、Dell Wyse Management Suite 跨站脚本漏洞。其中，“Dell PowerScale OneFS 默认密码漏洞、Dell PowerScale OneFS 整数溢出漏洞”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-2025-09394

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09398

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09397

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09396

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09399

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09680

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09679

https://www.cnvd.org.cn/flaw/show/CNVD-2025-09684

### 4、TOTOLINK 产品安全漏洞

TOTOLINK N150RT 是中国吉翁电子（TOTOLINK）公司的一款无线路由器。TOTOLINK AC1200 T8 和 AC1200 T10 是无线路由器设备。TOTOLINK AC1200 是中国吉翁电子（TOTOLINK）公司的一款双频 Wi-Fi 路由器。本周，上述产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞在系统上执行任意代码或者导致拒绝服务等。

CNVD 收录的相关漏洞包括：TOTOLINK N150RT /boafrm/formStaticDHCP 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formPortFw 文件缓冲区溢出漏洞、TOTO

LINK N150RT /boafrm/formWlwds 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formWdsEncrypt 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formVlan 文件缓冲区溢出漏洞、TOTOLINK AC1200 T8 和 AC1200 T10 cstecgi.cgi 文件 setParentalRules 函数缓冲区溢出漏洞、TOTOLINK AC1200 缓冲区溢出漏洞、TOTOLINK N150RT 命令注入漏洞（CNVD-2025-09944）。其中，除“TOTOLINK N150RT 命令注入漏洞（CNVD-2025-09944）”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-2025-09853
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09852
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09856
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09855
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09854
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09867
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09871
https://www.cnvd.org.cn/flaw/show/CNVD-2025-09944

**5、NETGEAR EX6120 sub_30394 函数缓冲区溢出漏洞**

NETGEAR EX6120 是美国网件（NETGEAR）公司的一款无线扩展器。本周，NETGEAR EX6120 被披露存在缓冲区溢出漏洞，该漏洞源于 sub_30394 函数参数 host 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。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-2025-09917

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-2025-09579 | Siemens SCALANCE LPE9403 SFTP 功能路径遍历漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-075201.html |
| CNVD-2025-09701 | lunary 跨站脚本漏洞 | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://github.com/lunary-ai/lunary/releases/tag/v1.2.29 |
| CNVD-2025 | Tenda W12/i24 缓冲区溢出漏 | 高 | 目前厂商已发布升级程序修复该安 |

| | | | |
|---|---|---|---|
| -09669 | 洞 | | 全问题，详情见厂商官网：https://www.tenda.com.cn/product/help/W12#download |
| CNVD-2025-09678 | GNU Mailman 命令注入漏洞 | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://list.org/download.html |
| CNVD-2025-09694 | NVIDIA ConnectX 权限问题漏洞 | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://nvidia.custhelp.com/app/answers/detail/a_id/5562 |
| CNVD-2025-09704 | lunary 访问控制错误漏洞（CNVD-2025-09704） | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://github.com/lunary-ai/lunary/commit/0755dde1afc2a74ec23b55eee03e4416916cf48f |
| CNVD-2025-09932 | Tenda RX2 Pro 信息泄露漏洞 | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://www.tendacn.com/us/download/detail-5715.html |
| CNVD-2025-09948 | Ivanti Endpoint Manager Mobile 代码执行漏洞 | 高 | Ivanti 已发布安全更新，用户应立即升级到修复版本：https://forums.ivanti.com/s/product-downloads |
| CNVD-2025-09703 | lunary 访问控制错误漏洞（CNVD-2025-09703） | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://github.com/lunary-ai/lunary/releases/tag/v1.2.29 |
| CNVD-2025-09945 | Tenda AC6 setDoublePppoeConfig 模块缓冲区溢出漏洞 | 高 | 目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://www.tendacn.com/download/detail-3794.html |

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞读取和写入任意文件，执行任意代码，导致内存破坏。此外，Microsoft、Dell、TOTOLINK 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，修改配置，在系统上执行任意代码，导致拒绝服务等。另外，NETGEAR EX6120 被披露存在缓冲区溢出漏洞，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。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 A810R 缓冲区溢出漏洞

**验证描述**

TOTOLINK A810R 是中国吉翁电子（TOTOLINK）公司的一款无线双频路由器。

TOTOLINK A810R 存在缓冲区溢出漏洞，该漏洞源于 downloadFile.cgi 中 v14 和 v3 参数未能正确验证输入数据的长度大小，远程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://locrian-lightning-dc7.notion.site/CVE-2025-28021-BufferOverflow1-1948e5e2b1a280e8aa5ad87964c5cd3d

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2025-09862

**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. iOS 内核漏洞公开 PoC 曝光：越狱与权限提升风险浮现

网络安全研究人员@karzan_0x455 近日公开了针对 CVE-2023-41992 漏洞的概念验证（PoC），该高危 iOS 内核漏洞虽已被苹果公司在 2023 年修复，但新披露的技术细节显示，恶意应用可能利用该漏洞绕过签名验证并提升权限。

参考链接：https://www.freebuf.com/articles/system/431339.html

### 2. Node.js 高危漏洞警报（CVE-2025-23166）：可导致远程系统崩溃

Node.js 团队近日发布重要安全公告，针对 24.x、23.x、22.x 和 20.x 版本系列推出关键更新。这些补丁修复了从低危到高危的一系列安全漏洞。

参考链接：https://www.freebuf.com/articles/system/431156.html

**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：010-82991783