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 13 日-2025 年 01 月 19 日 **2025 年第 3 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 453 个，其中高危漏洞 221 个、中危漏洞 206 个、低危漏洞 26 个。漏洞平均分值为 6.49。本周收录的漏洞中，涉及 0day 漏洞 331 个（占 73%），其中互联网上出现“Codezips Project Management System SQL 注入漏洞（CNVD-2025-00978）、XunRui CMS 跨站脚本漏洞”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 20278 个，与上周（6039 个）环比增多 236%。

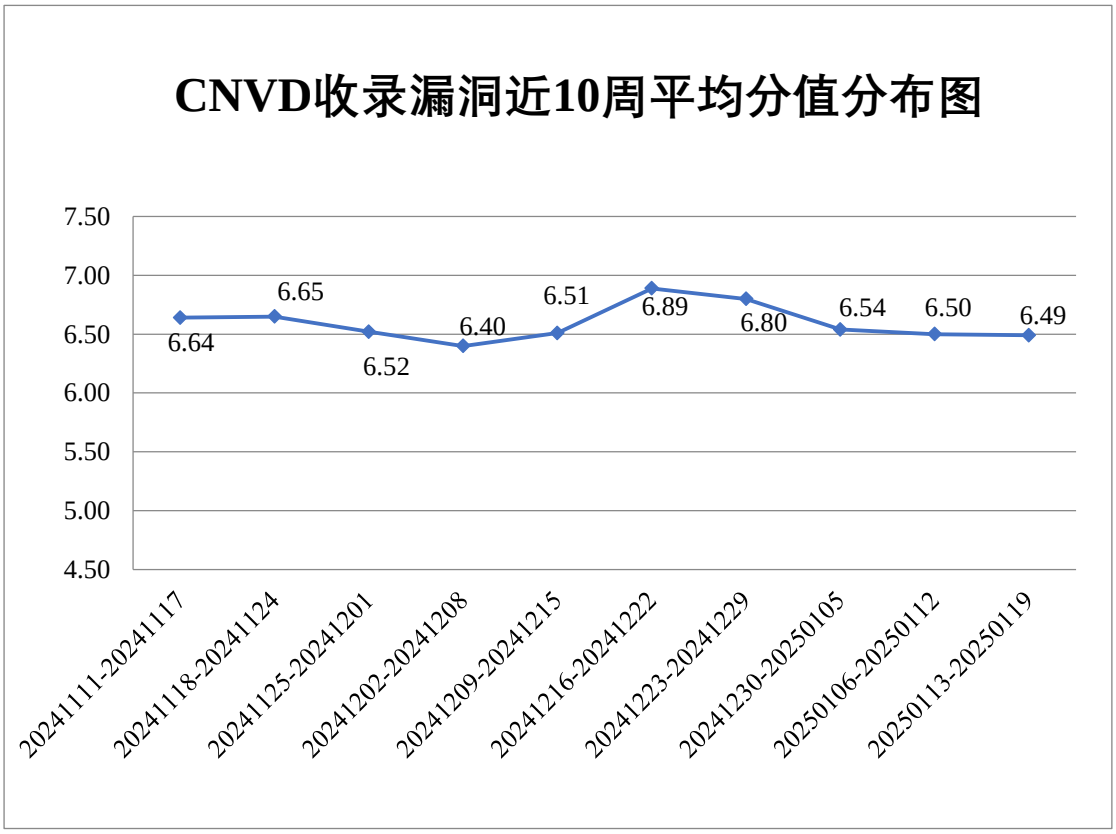

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 5 起，向基础电信企业通报漏洞事件 4 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 421 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 56 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 5 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：

昱能科技股份有限公司、北京安信立融科技股份有限公司、吉翁电子（深圳）有限公司、四平市九州易通科技有限公司、北京小桔科技有限公司、师创教育软件研究院（江苏）有限公司、天地伟业技术有限公司、北京好雨科技有限公司、公牛集团股份有限公司、北京金盘鹏图软件技术有限公司、深圳市吉祥腾达科技有限公司、普联技术有限公司、深圳国威电子有限公司、西安得买啦网络科技有限公司、畅捷通信息技术股份有限公司、深圳市必联电子有限公司、郑州微厦计算机科技有限公司、北京金和网络股份有限公司、北京派网软件有限公司、杭州达讯数字技术有限公司、北京神州视翰科技有限公司、上海真兰仪表科技股份有限公司、安徽旭帆信息科技有限公司、北京九思协同软件有限公司、用友网络科技股份有限公司、百度安全应急响应中心、浪潮工业互联网股份有限公司、广州红帆科技有限公司、安科瑞电气股份有限公司、统信软件技术有限公司、武汉达梦数据库有限公司、北京致远互联软件股份有限公司、佛山市杜特软件科技有限公司、北京华宇信息技术有限公司、青岛海信网络科技股份有限公司、青岛和正信息技术有限公司、广州网易计算机系统有限公司、漳州豆壳网络科技有限公司、成都飞鱼星科技股份有限公司、厦门网中网软件有限公司、北京星网锐捷网络技术有限公司、友讯电子设备（上海）有限公司、深圳市亿玛信诺科技有限公司、泛微网络科技股份有限公司、北京神州数码云计算有限公司、陕西不死鸟网络科技有限公司、智互联（深圳）科技有限公司、深圳市蓝凌软件股份有限公司、中版行知（广州）数字传媒有限公司、上海汉塔网络科技有限公司、北京通达信科科技有限公司、杭州雄伟科技开发股份有限公司、深圳市顶讯网络科技有限公司、腾讯音乐娱乐（深圳）有限公司、中电科金仓（北京）科技股份有限公司、北京奥博威斯科技有限公司、河南优卡助手信息技术有限公司、北京中科商软软件有限公司、广东顺景软件科技有限公司、重庆梅安森科技股份有限公司、北京国炬信息技术有限公司、江苏浪潮信息咨询有限公司、厦门四信通信科技有限公司、深圳市明源云科技有限公司、依米康科技集团股份有限公司、浙江大华技术股份有限公司、重庆旱獭信息技术有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、阿里云计算有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。江苏云天网络安全技术有限公司、北京纽盾网安信息技术有限公司、北京山石网科信息技术有限公司、江苏正信信息安全测试有限公司、江苏保旺达软件技术有限公司、统信软件技术有限公司、淮安易云科技有限公司、成都卫士通信息安全技术有限公司、中国电信股份有限公司上海研究院、含光实验室及其他个人白帽子向 CNVD 提交了 20278 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 20012 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）	18788	18788
三六零数字安全科技集团有限公司	1085	1085
新华三技术有限公司	999	0
深信服科技股份有限公司	791	0
安天科技集团股份有限公司	305	0
阿里云计算有限公司	163	1
上海交大	139	139
北京启明星辰信息安全技术有限公司	58	1
北京安信天行科技有限公司	49	49
南京众智维信息科技有限公司	37	9
杭州美创科技股份有限公司	13	13
北京长亭科技有限公司	6	0
北京天融信网络安全技术有限公司	3	3
江苏云天网络安全技术有限公司	18	18

北京纽盾网安信息技术有限公司	12	12
北京山石网科信息技术有限公司	12	12
江苏正信信息安全测试有限公司	6	6
西门子（中国）有限公司	5	0
江苏保旺达软件技术有限公司	4	4
统信软件技术有限公司	3	3
淮安易云科技有限公司	3	3
成都卫士通信息安全技术有限公司	3	3
中国电信股份有限公司上海研究院	1	1
含光实验室	1	1
个人	127	127
报送总计	22631	20278

本周漏洞按类型和厂商统计

本周，CNVD 收录了 453 个漏洞。WEB 应用 246 个，应用程序 91 个，网络设备（交换机、路由器等网络端设备）70 个，操作系统 31 个，数据库 7 个，智能设备（物联网终端设备）6 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
WEB 应用	246
应用程序	91
网络设备（交换机、路由器等网络端设备）	70
操作系统	31
数据库	7
智能设备（物联网终端设备）	6
安全产品	2

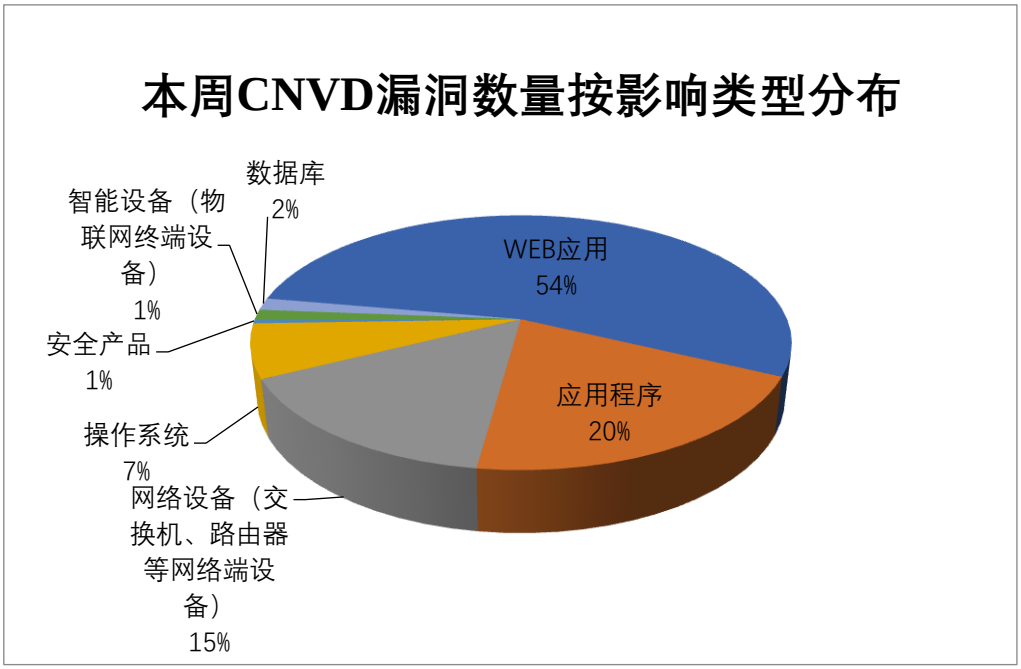

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、Linux、Foxit 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	用友网络科技股份有限公司	18	4%
2	Linux	15	3%
3	Foxit	12	3%
4	深圳市吉祥腾达科技有限公司	12	3%
5	D-Link	11	3%
6	Adobe	10	2%
7	Microsoft	10	2%
8	FFmpeg	10	2%
9	IBM	9	2%
10	其他	346	76%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，5 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Linksys E7350 vif_enable 命令注入漏洞、 Google Android prepare_to_draw_into_mask 任意代码执行漏洞”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/

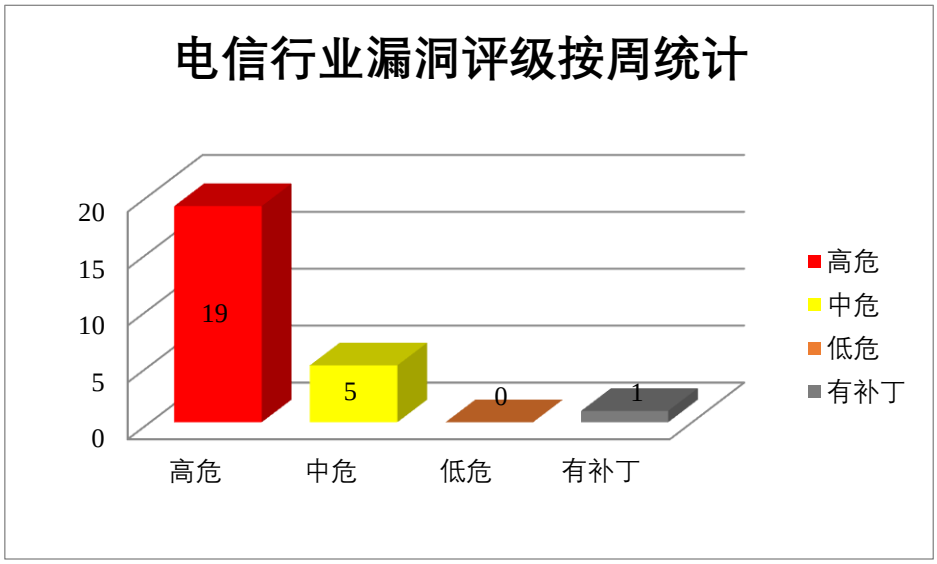

图 3 电信行业漏洞统计

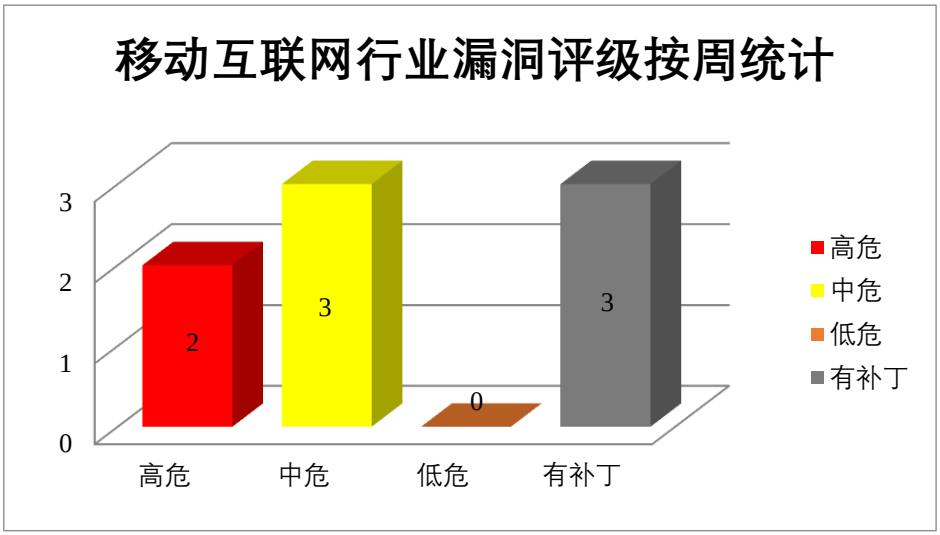

图 4 移动互联网行业漏洞统计

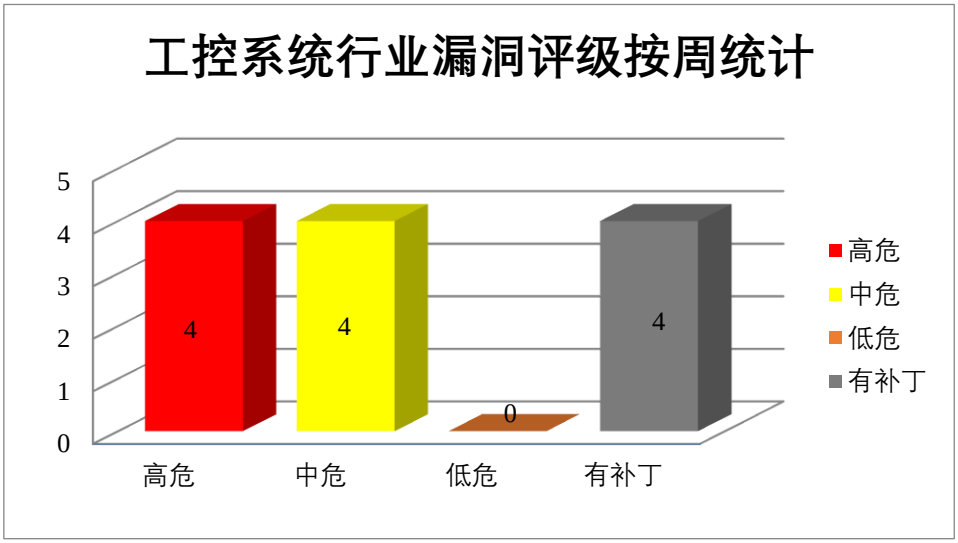

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows Remote Desktop Services 是美国微软（Microsoft）公司的一个允许用户远程访问图形桌面和 Windows 应用程序的功能集合。本周，上述产品被披露存在远程代码执行漏洞，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：Microsoft Windows Remote Desktop Services 远程代码执行漏洞（CNVD-2025-01185、CNVD-2025-01186、CNVD-2025-01187、CNVD-2025-01188、CNVD-2025-01189、CNVD-2025-01190、CNVD-2025-01191、CNVD-2025-01192）。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-2025-01185

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01186

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01187

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01188

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01189

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01190

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01191

https://www.cnvd.org.cn/flaw/show/CNVD-2025-01192

2、IBM 产品安全漏洞

IBM Engineering Lifecycle Optimization - Engineering Insights（简称 ENI）是 IBM 提供的一款协作型、基于 Web 的应用程序。IBM AIX 是美国国际商业机器（IBM）

公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM WebSphere Automation 是 IBM 公司的一款自动化管理软件，用于优化和管理数据中心资源。IBM Storage Scale 是美国国际商业机器（IBM）公司的一个存储解决方案，旨在帮助企业有效地管理和扩展存储资源，满足不断增长的数据存储需求。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 Protect（IBM Spectrum Protect）是美国国际商业机器（IBM）公司的一款备份软件。为物理文件服务器、虚拟环境和各种应用程序提供全面的数据数据灾备能力。IBM Security QRadar 是美国国际商业机器（IBM）公司的一个现代化的威胁检测和响应解决方案。旨在统一整合安全分析师体验，提高他们在整个事件生命周期中的响应速度。IBM Workload Scheduler 是美国国际商业机器（IBM）公司的一套企业任务调度软件。该软件能够自动化控制工作负载。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，注入恶意 HTML 代码，执行非法 SQL 命令窃取数据库敏感数据，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Engineering Lifecycle Optimization-Engineering Insights 信息泄露漏洞、IBM AIX 竞争条件问题漏洞、IBM WebSphere Automation 命令注入漏洞、IBM Storage Scale SQL 注入漏洞、IBM Cognos Analytics 文件上传漏洞（CNVD-2025-00968）、IBM Storage Protect 授权问题漏洞、IBM Security Qradar HTML 注入漏洞、IBM Workload Scheduler 信息泄露漏洞。其中，“IBM WebSphere Automation 命令注入漏洞、IBM Storage Scale SQL 注入漏洞、IBM Cognos Analytics 文件上传漏洞（CNVD-2025-00968）”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-2025-00967
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00966
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00965
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00970
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00968
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00973
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00972
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00971

3、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

漏洞在受害者的浏览器会话中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-01174、CNVD-2025-01175、CNVD-2025-01176、CNVD-2025-01177、CNVD-2025-01178、CNVD-2025-01179、CNVD-2025-01180、CNVD-2025-01181）。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-2025-01174
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01175
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01176
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01177
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01178
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01179
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01180
https://www.cnvd.org.cn/flaw/show/CNVD-2025-01181

4、 Foxit 产品安全漏洞

Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 阅读器。Foxit PDF Editor 是中国福昕（Foxit）公司的一款 PDF 编辑器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞诱导用户打开恶意文件或恶意页面后导致恶意代码执行。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2025-00954、CNVD-2025-00964）、Foxit PDF Editor 缓冲区溢出漏洞（CNVD-2025-00958、CNVD-2025-00961、CNVD-2025-00960、CNVD-2025-00959、CNVD-2025-00963、CNVD-2025-00962）。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-2025-00954
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00958
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00961
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00960
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00959
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00964
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00963
https://www.cnvd.org.cn/flaw/show/CNVD-2025-00962

5、 Siemens SIPROTEC 5 文件访问限制不当漏洞

SIPROTEC 5 设备为变电站和其他应用领域提供一系列集成保护、控制、测量和自动化功能。本周，Siemens SIPROTEC 5 被披露存在文件访问限制不当漏洞，攻击者可利用该漏洞读取任意文件或设备的整个文件系统。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-2025-01697

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-2025-00984	Rockwell Automation FactoryTalk Transaction Manager 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139744
CNVD-2025-01606	huawei HarmonyOS 权限许可和访问控制问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2025/1/
CNVD-2025-01605	Huawei HarmonyOS 信息泄露漏洞（CNVD-2025-01605）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2025/1/
CNVD-2025-01659	Siemens Mendix LDAP 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://marketplace.mendix.com/link/component/210270
CNVD-2025-01668	SonicWall SonicOS 堆栈溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0004
CNVD-2025-01689	FFmpeg 缓冲区溢出漏洞（CNVD-2025-01689）	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://ffmpeg.org/download.html
CNVD-2025-01691	SonicWALL SonicOS IPSec VPN 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0012
CNVD-2025-01694	Ffmpeg 资源管理错误漏洞（CNVD-2025-01694）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/cc867f2c09d2b69cee8a0eccd62aff002cbbfe11
CNVD-2025-01667	Linksys E7350 vif_enable 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://support.linksys.com/kb/article/

			6935-cn/
CNVD-2025-00964	Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2025-00964）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html

小结：本周，Microsoft 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。此外，IBM、Adobe、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敏感信息，注入恶意 HTML 代码，执行非法 SQL 命令窃取数据库敏感数据，在系统上执行任意代码等。另外，Siemens SIPROTEC 5 被披露存在文件访问限制不当漏洞，攻击者可利用该漏洞读取任意文件或设备的整个文件系统。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、XunRui CMS 跨站脚本漏洞

验证描述

XunRui CMS（迅睿 CMS）是中国迅睿（Xunrui）公司的一套开源的内容管理系统（CMS）。

XunRui CMS v4.6.1 版本存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，远程攻击者可利用该漏洞通过项目设置页签中的项目名称功能执行任意代码。

验证信息

POC 链接：https://github.com/Cosemz/CVE/blob/main/xunruicms/XunRuiCms%20Stored%20XSS%20%28Authenticated%29.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2025-00979

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. 微软活动目录组策略存在重大漏洞，NTLMv 身份验证可被绕过

Silverfort 的网络安全研究团队发现微软活动目录组策略存在一个重大缺陷，即使表

面上已禁用，仍允许 NTLMv1 身份验证持续存在。

参考链接：https://cybersecuritynews.com/active-directory-group-policy-bypassed/#google_vignette

2. MikroTik 僵尸网络依赖 DNS 配置错误来传播恶意软件

Infoblox 研究人员发现了一个由 13000 台 MikroTik 设备组成的僵尸网络，这些设备利用 DNS 错误配置来绕过电子邮件保护，欺骗大约 20000 个域并传播恶意软件。

参考链接：https://securityaffairs.com/173126/hacking/13000-device-mikrotik-botnet-exploiting-dns-flaws.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：010-82991537