国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 11 月 04 日-2024 年 11 月 10 日 **2024 年第 45 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 230 个，其中高危漏洞 99 个、中危漏洞 122 个、低危漏洞 9 个。漏洞平均分值为 6.44。本周收录的漏洞中，涉及 0day 漏洞 148 个（占 64%），其中互联网上出现“D-Link DIR-619L 缓冲区溢出漏洞（CNVD-2024-43210）、AutoCMS SQL 注入漏洞”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 6618 个，与上周（9485 个）环比减少 30%。

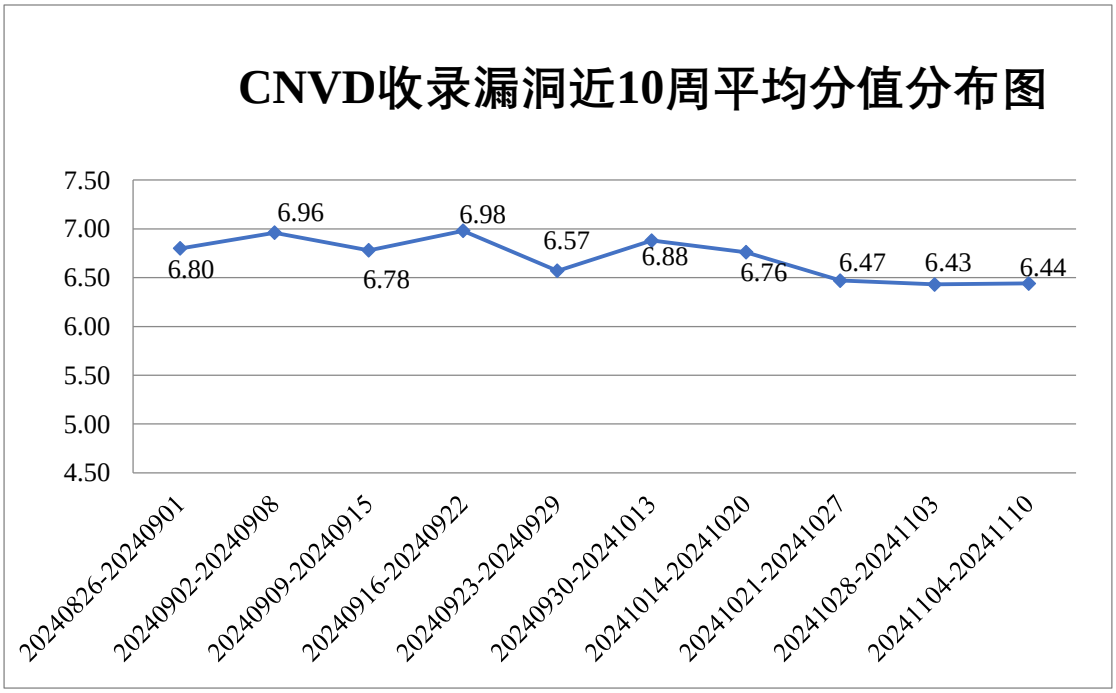

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 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 485 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 20 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：

紫光软件系统有限公司、重庆紫光华智科技有限公司、智互联（深圳）科技有限公司、浙江兰德纵横网络技术股份有限公司、用友网络科技股份有限公司、夏普商贸（中国）有限公司、西安紫云羚网络科技有限责任公司、武汉天地伟业科技有限公司、土流集团有限公司、天津南大通用数据技术股份有限公司、苏州能加信息技术有限公司、苏州汉明科技有限公司、施耐德电气（中国）有限公司、神州数码控股有限公司、深圳市雄帝科技股份有限公司、深圳市赛格导航科技股份有限公司、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、深圳市汇川技术股份有限公司、深圳市顶讯网络科技有限公司、深圳市北斗云信息技术有限公司、深圳华颐智能系统有限公司、深信服科技股份有限公司、上海卓卓网络科技有限公司、上海派拉软件技术有限公司、上海泛微网络科技股份有限公司、上海北塔软件股份有限公司、上海百胜软件股份有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、容知日新科技股份有限公司、青岛东软载波科技股份有限公司、南北天地科技股份有限公司、龙采科技集团有限责任公司、廊坊市极致网络科技有限公司、柯尼卡美能达集团、吉翁电子（深圳）有限公司、河南英才归来科技有限公司、合肥贰道网络科技有限公司、汉王科技股份有限公司、广州市天翎网络科技有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、福建万福信息技术有限公司、泛微网络科技股份有限公司、东莞市广义信息科技有限公司、畅捷通信息技术股份有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京小桔科技有限公司、北京万户软件技术有限公司、北京神州数码云计算有限公司、北京神州视翰科技有限公司、北京雷石天地电子技术有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京嘉华汇诚科技股份有限公司、北京华志信科技股份有限公司、北京浩鸿达科技发展股份公司和奥琦玮信息科技（北京）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、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、深信服科技股份有限公司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、河南东方云盾信息技术有限公司、江苏云天网络安全技术有限公司、江苏金盾检测技术股份有限公司、北京网御星云信息技术有限公司、上海维信荟智金融科技有限公司、北京纽盾网安信息技术有限公司、上海谋乐网络科技有限公司、北京安帝科技有限公司、北京中睿天下信息技术有限公司、北京山石网科信息技术有限公司、北京翰慧投资咨询有限公司、联通数字科技有限公司、北京时代新威信息技术有限公司、上海观安信息技术股份有限公司、上海亿保健康科技集团有限公司、卫士通（广州）信息安全技术有限公司、淮安易云科技有限公司、成都安美勤信息技术股份有限公司、北京航空航天大学、北京君云天下科技有限公司、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、深圳昂楷科技有限公司、北京天下信安技术有限公司、中资网络信息安全科技有限公司、浙江国利网安科技有限公司、电子科技大学公共安全信息与装备集成技术研究中心、江苏晟晖信息科技有限公司、深圳市佰航信息技术有限公司、江苏正信信息安全测试有限公司、中华人民共和国上海海事局、北京比瓴科技有限公司、上海蜚语信息科技有限公司、国核自仪网络安全技术（上海）有限责任公司及其他个人白帽子向 CNVD 提交了 6618 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 5122 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）	4366	4366
天津市国瑞数码安全系统股份有限公司	3019	0
北京天融信网络安全技术有限公司	2134	20
北京神州绿盟科技有限公司	1466	136
新华三技术有限公司	603	0
三六零数字安全科技集团有限公司	554	554
深信服科技股份有限公司	531	5
安天科技集团股份有限公司	355	48
上海交大	202	202
阿里云计算有限公司	166	0
南京众智维信息科技	125	8

有限公司		
北京知道创宇信息技术有限公司	109	2
北京安信天行科技有限公司	91	91
北京启明星辰信息安全技术有限公司	84	22
恒安嘉新（北京）科技股份公司	28	0
北京数字观星科技有限公司	28	0
快页信息技术有限公司	17	17
北京长亭科技有限公司	17	1
京东科技信息技术有限公司	16	16
远江盛邦（北京）网络安全科技股份有限公司	15	15
华为技术有限公司	10	10
杭州迪普科技股份有限公司	10	0
杭州美创科技股份有限公司	10	10
北京升鑫网络科技有限公司（青藤云）	10	10
杭州安恒信息技术股份有限公司	2	2
北京信联数安科技有限公司	2	2
成都卫士通信息安全技术有限公司	49	49
河南东方云盾信息技术有限公司	32	32

江苏云天网络安全技术有限公司	15	15
江苏金盾检测技术股份有限公司	14	14
北京网御星云信息技术有限公司	12	12
上海维信荟智金融科技有限公司	11	11
北京纽盾网安信息技术有限公司	11	11
上海谋乐网络科技有限公司	10	10
北京安帝科技有限公司	8	8
北京中睿天下信息技术有限公司	7	7
北京山石网科信息技术有限公司	7	7
北京翰慧投资咨询有限公司	7	7
联通数字科技有限公司	6	6
北京时代新威信息技术有限公司	6	6
上海观安信息技术股份有限公司	4	4
上海亿保健康科技集团有限公司	4	4
卫士通（广州）信息安全技术有限公司	3	3
淮安易云科技有限公司	3	3
成都安美勤信息技术股份有限公司	3	3
北京航空航天大学	2	2

北京君云天下科技有限公司	2	2
亚信科技（成都）有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
深圳昂楷科技有限公司	2	2
北京天下信安技术有限公司	2	2
中资网络信息安全科技有限公司	1	1
浙江国利网安科技有限公司	1	1
电子科技大学公共安全信息与装备集成技术研究中心	1	1
江苏晟晖信息科技有限公司	1	1
深圳市佰航信息技术有限公司	1	1
江苏正信信息安全测试有限公司	1	1
中华人民共和国上海海事局	1	1
北京比瓴科技有限公司	1	1
上海蜚语信息科技有限公司	1	1
国核自仪网络安全技术（上海）有限责任公司	1	1
CNCERT 宁夏分中心	22	22
个人	825	825
报送总计	15051	6618

本周漏洞按类型和厂商统计

本周，CNVD 收录了 230 个漏洞。WEB 应用 114 个，应用程序 49 个，网络设备（交换机、路由器等网络端设备）41 个，安全产品 12 个，智能设备（物联网终端设备）10 个，数据库 4 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	114
应用程序	49
网络设备（交换机、路由器等网络端设备）	41
安全产品	12
智能设备（物联网终端设备）	10
数据库	4

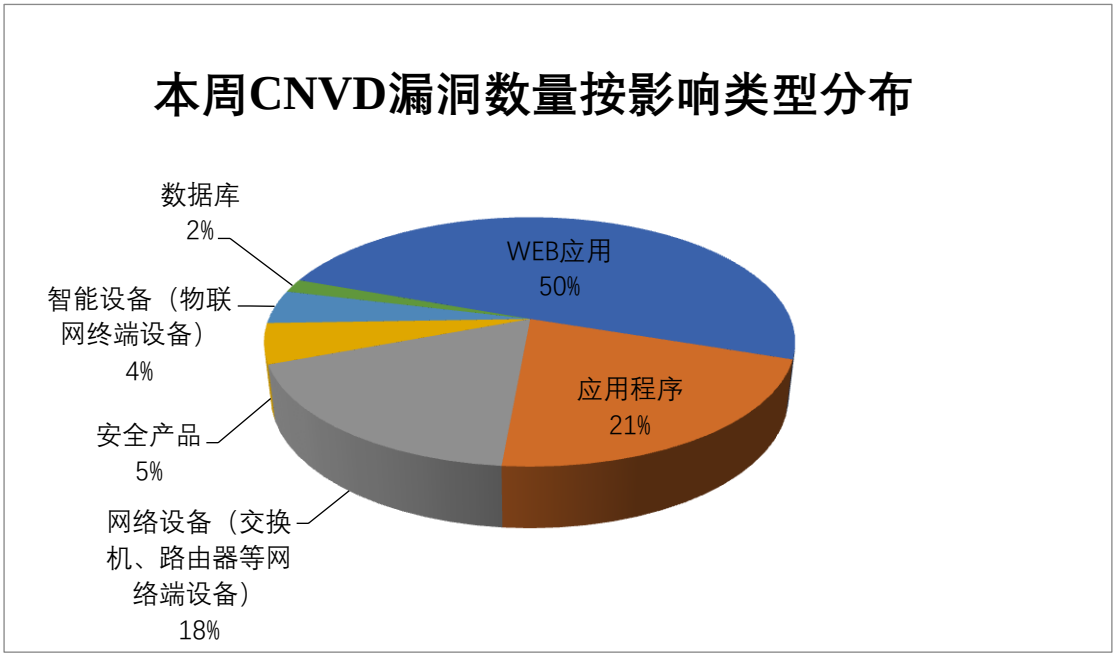

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、用友网络科技股份有限公司、Microsoft 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	IBM	19	8%
2	用友网络科技股份有限公司	14	6%
3	Microsoft	11	5%

4	NETGEAR	10	4%
5	Adobe	10	4%
6	Cisco	9	4%
7	Mitel	9	4%
8	TRENDnet	6	3%
9	北京神州视翰科技有限公司	6	3%
10	其他	136	59%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，4 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“NETGEAR R8500 admin_account.cgi 组件命令注入漏洞、IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2024-43189）”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/

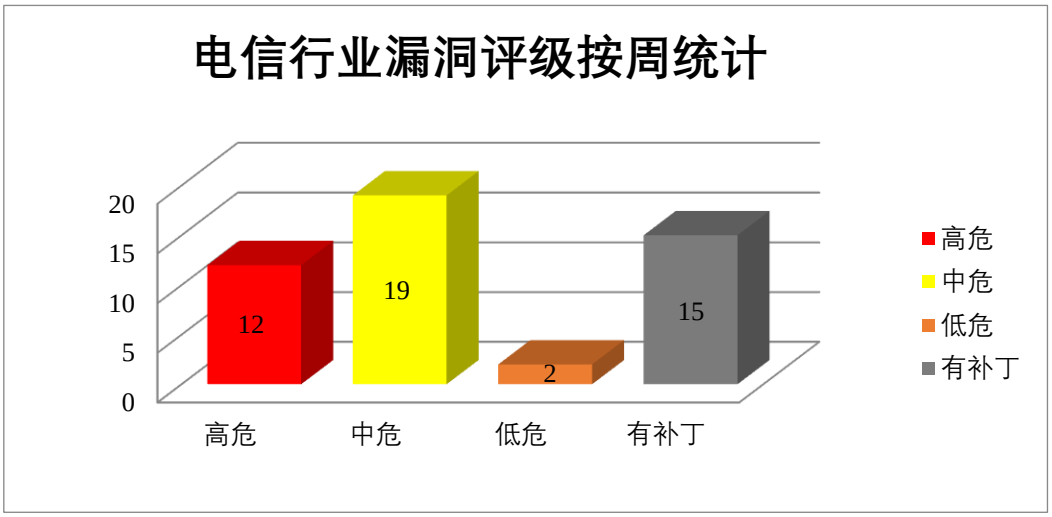

图 3 电信行业漏洞统计

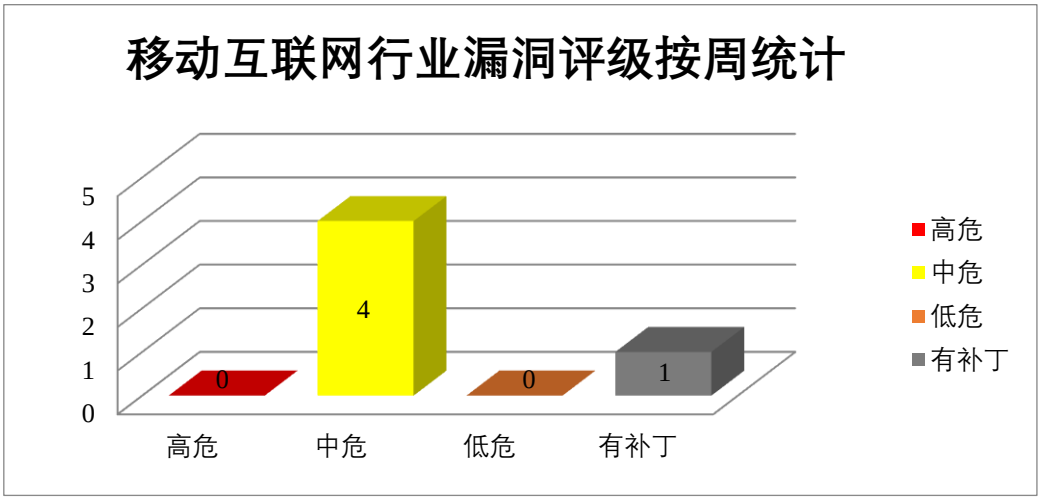

图 4 移动互联网行业漏洞统计

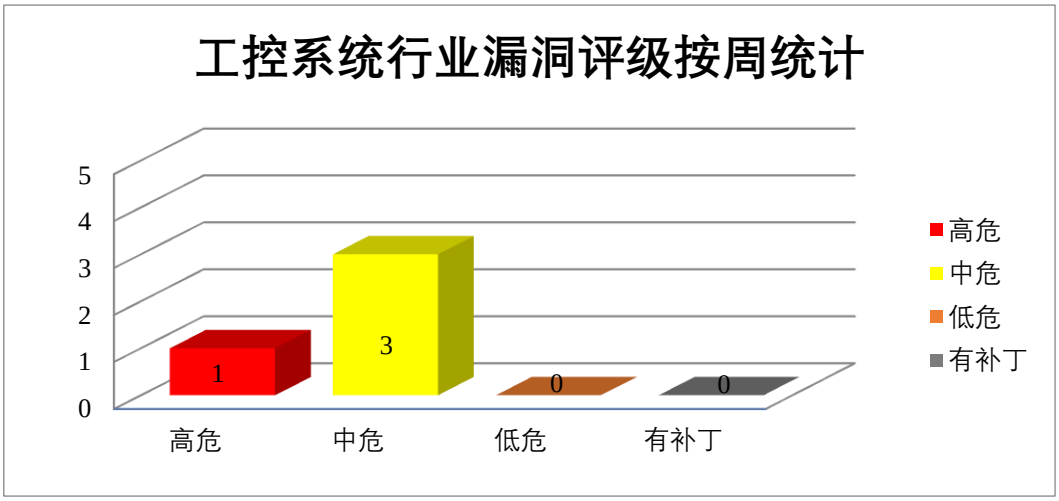

图 5 工控系统行业漏洞统计

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 Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Dimension 是一套 2D 和 3D 合成设计工具。Adobe Media Encoder 是一款音、视频编码应用程序。Adobe Illustrator 是一套基于向量的图像制作软件。Adobe Premiere Pro 是一套非线性编辑的视频剪辑软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，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 Acrobat Reader 资源管理错误漏洞（CNVD-2024-43036、CNVD-2024-43038、CNVD-2024-43037）、Adobe Dimension 资源管理错误漏洞（CNVD-2024-43040）、Adobe Media Encoder 缓冲区溢出漏洞（CNVD-2024-43043）、Adobe Illustrator 资源管理错误漏洞（CNVD-2024-43042）、Adobe Premiere Pro 缓冲区溢出漏洞（CNVD-2024-43045、CNVD-2024-43044）。其中，除“Adobe Pre

miere Pro 缓冲区溢出漏洞（CNVD-2024-43045）”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-2024-43036
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43040
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43038
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43037
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43043
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43042
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43045
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43044

2、 Cisco 产品安全漏洞

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞执行任意脚本代码，访问基于浏览器的敏感信息。

CNVD 收录的相关漏洞包括：Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2024-43201、CNVD-2024-43204、CNVD-2024-43203、CNVD-2024-43202、CNVD-2024-43207、CNVD-2024-43206、CNVD-2024-43205、CNVD-2024-43209）。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-2024-43201
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43204
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43203
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43202
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43207
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43206
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43205
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43209

3、 IBM 产品安全漏洞

IBM WebSphere Application Server（WAS）是美国国际商业机器（IBM）公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。IBM Watson Studio Local 是一套协作数据处理解决方案。该产品包括数据分析、数据可视化、数据清理和流数据提取等功能。 IBM Sterling Connect: Direct Web Services 是一套基于文件的点对点文件传输解决方案。IBM OpenBMC 是一个 Linux 发行版，用于管理服务器、架顶式交换机或 RAID 设备等设备的控制器。IBM

Db2 是一套关系型数据库管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在 Web UI 中嵌入任意 JavaScript 代码，获取敏感信息或消耗内存资源，使用特制查询，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 代码问题漏洞（CNVD-2024-43186）、IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2024-43189）、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2024-43188）、IBM Watson Studio Local 跨站请求伪造漏洞、IBM Sterling Connect:Direct Web Services 加密问题漏洞、IBM OpenBMC 权限提升漏洞、IBM Db2 注入漏洞、IBM Db2 拒绝服务漏洞（CNVD-2024-43199）。其中，“IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2024-43189）、IBM OpenBMC 权限提升漏洞”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-2024-43186
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43189
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43188
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43187
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43192
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43195
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43200
https://www.cnvd.org.cn/flaw/show/CNVD-2024-43199

4、Microsoft 产品安全漏洞

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 Office Visio 是 Office 软件系列中的负责绘制流程图和示意图的软件。Microsoft Office PowerPoint 是一个用于制作、演示文稿（PPT）的软件。Microsoft Office OneNote 是一套用于自由形式的信息获取以及多用户协作工具。Microsoft Excel 是一款 Office 套件中的电子表格处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Office Visio 远程代码执行漏洞（CNVD-2024-42939）、Microsoft Office 远程代码执行漏洞（CNVD-2024-42940、CNVD-2024-42942）、Microsoft Office 欺骗漏洞（CNVD-2024-42941）、Microsoft Office PowerPoint 资源管理错误漏洞、Microsoft Office OneNote 远程代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2024-42947）、Microsoft Excel 权限提升漏洞（CNVD-2024-42948）。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-2024-42939
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42940
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42941
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42942
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42943
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42946
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42947
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42948

5、Tenda AX2 Pro 操作系统命令注入漏洞

Tenda AX2 Pro 是中国腾达（Tenda）公司的一款家庭用户设计入门级的千兆 Wi-Fi 6 路由器。本周，Tenda AX2 Pro 被披露存在操作系统命令注入漏洞。攻击者可利用该漏洞通过构建恶意有效负载来执行命令。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-2024-43212

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-2024-42930	Mitel MiCollab SQL 注入漏洞（CNVD-2024-42930）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0028
CNVD-2024-42932	Mitel MiCollab SQL 注入漏洞（CNVD-2024-42932）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0004
CNVD-2024-42931	Mitel MiCollab 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://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0013
CNVD-2024-42934	Mitel MiCollab SQL 注入漏洞（CNVD-2024-42934）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0004
CNVD-2024	Mitel MiCollab SQL 注入漏	高	厂商已发布了漏洞修复程序，请及

-42937	洞（CNVD-2024-42937）		时关注更新：https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0014
CNVD-2024-42945	Microsoft Office 欺骗漏洞（CNVD-2024-42945）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200
CNVD-2024-42948	Microsoft Excel 权限提升漏洞（CNVD-2024-42948）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465
CNVD-2024-43043	Adobe Media Encoder 缓冲区溢出漏洞（CNVD-2024-43043）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/media-encoder/apsb21-118.html
CNVD-2024-43189	IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2024-43189）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7173263
CNVD-2024-43038	Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-43038）	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/acrobat/apsb24-29.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在当前用户的上下文中执行任意代码。此外，Cisco、IBM、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问基于浏览器的敏感信息，在 Web UI 中嵌入任意 JavaScript 代码，使用特制查询，导致拒绝服务，在系统上执行任意代码等。另外，Tenda AX2 Pro 被披露存在操作系统命令注入漏洞。攻击者可利用漏洞通过构建恶意有效负载来执行命令。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、AutoCMS SQL 注入漏洞

验证描述

AutoCMS 是 AutoCMS 开源的一个内容管理系统（CMS）。可帮助经销商管理其网站内容、在线广告、社交媒体和分析。

AutoCMS 5.4 版本存在 SQL 注入漏洞，该漏洞源于/admin/robot.php 的侧边栏参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库

敏感数据。

验证信息

POC 链接：https://github.com/Hebing123/cve/issues/69

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-43215

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. Whitehat 发现漏洞，该漏洞允许超过 7 亿个 EA 帐户进行未经授权的访问

游戏开发人员和逆向工程师 Sean Kahler 设法在未经授权的情况下访问了超过 7 亿个 Electronic Arts（EA）用户帐户，包括游戏统计数据。白帽帮助修补了这个关键缺陷。

参考链接：https://cybernews.com/security/whitehat-gains-access-to-over-700-million-ea-accounts/

2. Ollama AI 模型发现六个漏洞，能导致 DoS 攻击、模型中毒

网络安全研究人员披露了 Ollama 人工智能模型中的六个安全漏洞，攻击者可能会利用这些漏洞执行各种操作。

参考链接：https://www.freebuf.com/news/414559.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