国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 03 月 11 日-2024 年 03 月 17 日 **2024 年第 11 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 438 个，其中高危漏洞 166 个、中危漏洞 254 个、低危漏洞 18 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 356 个（占 81%），其中互联网上出现“XunRuiCMS 跨站脚本漏洞（CNVD-2024-12713）、CMS Made Simple 跨站脚本漏洞（CNVD-2024-13561）”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事件型漏洞总数 12519 个，与上周（9326 个）环比增加 34%。

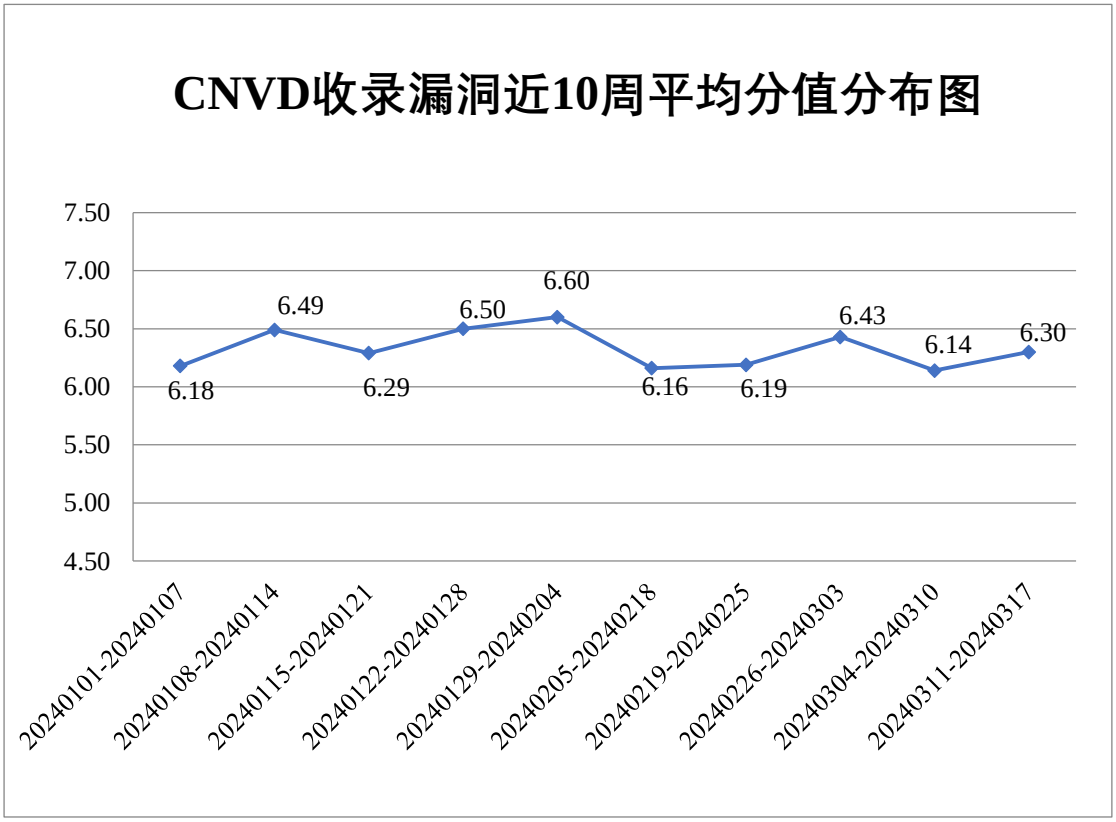

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 832 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 187 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 44 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：

佐藤自动识别系统国际贸易（上海）有限公司、卓智网络科技有限公司、珠海奔图打印科技有限公司、重庆中联信息产业有限责任公司、中码科技发展（成都）有限公司、中控技术股份有限公司、智慧芽信息科技（苏州）有限公司、智互联（深圳）科技有限公司、正方软件股份有限公司、浙江兰德纵横网络技术股份有限公司、浙江华途信息安全技术股份有限公司、浙江华锐捷技术有限公司、浙江花田网络有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、雅马哈乐器音响（中国）投资有限公司、兄弟（中国）商业有限公司、新晨科技股份有限公司、鲜丰水果股份有限公司、西安海内教育科技有限公司、武汉中地数码科技有限公司、武汉星巡智能科技有限公司、武汉达梦数据库有限公司、威海市天罡仪表股份有限公司、网件（北京）网络技术有限公司、万洲电器股份有限公司、万洲电气股份有限公司、天津华春智慧能源科技发展有限公司、天津黑核科技有限公司、泰华智慧产业集团股份有限公司、台铃科技股份有限公司、苏州赛分科技股份有限公司、苏州汉明科技有限公司、四川奇石缘科技股份有限公司、深圳坐标软件集团有限公司、深圳智慧光迅信息技术有限公司、深圳维盟科技股份有限公司、深圳市中电电力技术股份有限公司、深圳市智百威科技发展有限公司、深圳市信特安科技有限公司、深圳市图美电子技术有限公司、深圳市拓普泰尔科技有限公司、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、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市华旭科技开发集团、深圳市单仁牛商科技股份有限公司、深圳市爱德数智科技股份有限公司、深圳华视美达信息技术有限公司、上海卓卓网络科技有限公司、上海正品贵德软件有限公司、上海曼恒数字技术股份有限公司、上海灵当信息科技有限公司、上海惠诚科教器械股份有限公司、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、上海繁易信息科技股份有限公司、上海创旗天下科技股份有限公司、上海伯俊软件科技有限公司、熵基科技股份有限公司、商派软件有限公司、山脉科技股份有限公司、山东威尔数据股份有限公司、山东泰港数字科技集团有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、润申标准化技术服务（上海）有限公司、任子行网络技术股份有限公司、青岛自贸供应链管理有限公司、青岛海信网络科技股份有限公司、青岛东胜伟业软件有限公司、启明信息技术股份有限公司、南京千目信息科

技有限公司、纳龙健康科技股份有限公司、明腾网络股份有限公司、洛阳硕力信新能源科技有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、浪潮数字（山东）科技有限公司、朗坤智慧科技股份有限公司、蓝网科技股份有限公司、昆明天宏网络科技有限公司、济南聚易信息技术有限公司、吉翁电子（深圳）有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、淮南市银泰软件科技有限公司、华新智科技产业发展股份有限公司、湖南壹拾捌号网络技术有限公司、湖南强智科技发展有限公司、湖北叶威（集团）智能科技有限公司、宏脉信息技术（广州）股份有限公司、杭州西软信息技术有限公司、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、杭州安恒信息技术股份有限公司、海南新南宝商用设备有限公司、哈尔滨新中新电子股份有限公司、广州图创计算机软件开发有限公司、广州同鑫科技有限公司、广州市保伦电子有限公司、广东保伦电子股份有限公司、福建星网锐捷通讯股份有限公司、福建科立讯通信有限公司、帆软软件有限公司、东莞市通天星软件科技有限公司、单县自由仁网络技术开发工作室、大唐电信科技股份有限公司、成都智蜂网科技有限责任公司、成都天问互联科技有限公司、成都市任我行信息技术有限公司、北京中远麒麟科技有限公司、北京中农信达信息技术有限公司、北京中科聚网信息技术有限公司、北京中科金马科技股份有限公司、北京长天科创信息技术有限公司、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、北京网达立信信息技术有限公司、北京万户网络技术有限公司、北京数码大方科技股份有限公司、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、北京金和网络股份有限公司、北京慧图（集团）科技股份有限公司、北京国基科技股份有限公司、北京博胜神舟科技有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安吉加加信息技术有限公司、爱普生（中国）有限公司、YeaLink 和 NVIDIA。

本周，CNVD 发布了《Microsoft 发布 2024 年 3 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9826

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、天津市国瑞数码安全系统股份有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。江苏金盾检测技术股份有限公司、河南东方云盾信息技术有限公司、联想集团、贵州多彩网安科技有限公司、快页信息技术有限公司、北京时代新威信息技术有限公司、吉林省吉林祥云信息技术有限公司、中国电信股份有限公司上海研究院、北京远禾科技有限公司、内蒙古中叶信息技

术有限责任公司、中资网络信息安全科技有限公司、甘肃赛飞安全科技有限公司、北京微步在线科技有限公司、中孚安全技术有限公司、山石网科通信技术股份有限公司、中电万维信息技术有限责任公司、广西塔易信息技术有限公司、江苏天竞云合数据技术有限公司、江苏天创科技有限公司、内蒙古洞明科技有限公司、河南灵创电子科技有限公司、上海观安信息技术股份有限公司、西藏熙安信息技术有限责任公司、上海直画科技有限公司、湖南泛联新安信息科技有限公司、北京山石网科信息技术有限公司、人保信息科技有限公司、中国电信股份有限公司研究院及其他个人白帽子向 CNVD 提交了 12519 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）、奇安信网神（补天平台）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 11375 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）	8340	8340
奇安信网神（补天平台）	1137	1137
新华三技术有限公司	1135	0
上海交大	1100	1100
三六零数字安全科技集团有限公司	798	798
天津市国瑞数码安全系统股份有限公司	362	0
北京神州绿盟科技有限公司	296	0
安天科技集团股份有限公司	239	0
北京天融信网络安全技术有限公司	194	0
北京启明星辰信息安全技术有限公司	158	5
恒安嘉新(北京)科技股份公司	80	0
中电科网络安全科技股份有限公司	78	0
杭州安恒信息技术股份有限公司	75	2

中国电信集团系统集成有限责任公司	61	0
北京安信天行科技有限公司	33	33
北京数字观星科技有限公司	13	0
杭州迪普科技股份有限公司	10	0
远江盛邦（北京）网络安全科技股份有限公司	10	10
北京长亭科技有限公司	4	2
浙江大华技术股份有限公司	1	1
北京智游网安科技有限公司	1	1
江苏金盾检测技术股份有限公司	65	65
河南东方云盾信息技术有限公司	38	38
联想集团	23	23
贵州多彩网安科技有限公司	21	21
西门子（中国）有限公司	11	0
快页信息技术有限公司	11	11
北京时代新威信息技术有限公司	10	10
吉林省吉林祥云信息技术有限公司	9	9
中国电信股份有限公司上海研究院	8	8
北京远禾科技有限公	8	8

司		
内蒙古中叶信息技术有限责任公司	7	7
中资网络信息安全科技有限公司	6	6
甘肃赛飞安全科技有限公司	6	6
北京微步在线科技有限公司	6	6
中孚安全技术有限公司	6	6
山石网科通信技术股份有限公司	3	3
中电万维信息技术有限责任公司	3	3
广西塔易信息技术有限公司	2	2
江苏天竞云合数据技术有限公司	2	2
江苏天创科技有限公司	2	2
内蒙古洞明科技有限公司	2	2
河南灵创电子科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
西藏熙安信息技术有限责任公司	1	1
上海直画科技有限公司	1	1
湖南泛联新安信息科技有限公司	1	1
北京山石网科信息技术有限公司	1	1

人保信息科技有限公司	1	1
中国电信股份有限公司研究院	1	1
个人	842	842
报送总计	15226	12519

本周漏洞按类型和厂商统计

本周，CNVD 收录了 438 个漏洞。WEB 应用 223 个，应用程序 141 个，网络设备（交换机、路由器等网络端设备）37 个，智能设备（物联网终端设备）20 个，操作系统 7 个，安全产品 4 个，数据库 4 个，车联网 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	223
应用程序	141
网络设备（交换机、路由器等网络端设备）	37
智能设备（物联网终端设备）	20
操作系统	7
安全产品	4
数据库	4
车联网	2

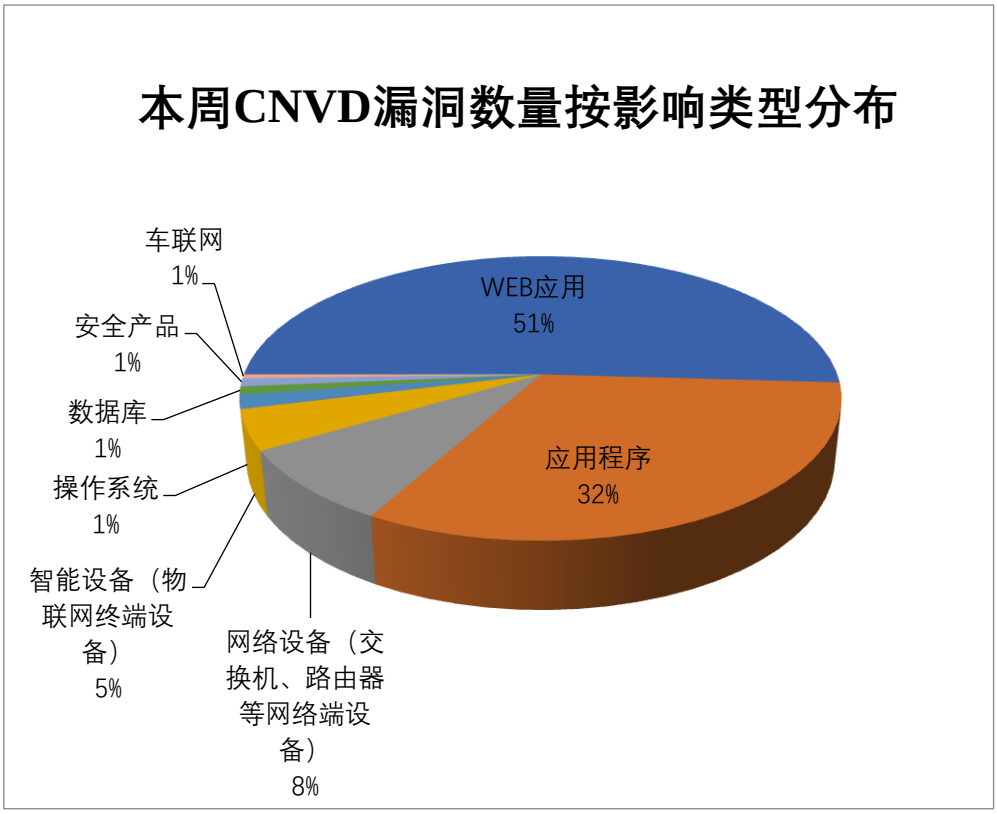

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Kashipara、IBM、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	Kashipara	19	4%
2	IBM	13	3%
3	北京星网锐捷网络技术有限公司	12	3%
4	Fortinet	12	3%
5	Adobe	11	3%
6	mozilla	10	2%
7	用友网络科技股份有限公司	9	2%
8	北京亿赛通科技发展有限责任公司	9	2%
9	浙江大华技术股份有限公司	8	2%
10	其他	335	76%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，59 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“多款 Fortinet 产品格式化字符串错误漏洞（CNVD-2024-13095）、TP-LINK ER7206 操作系统命令注入漏洞”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/

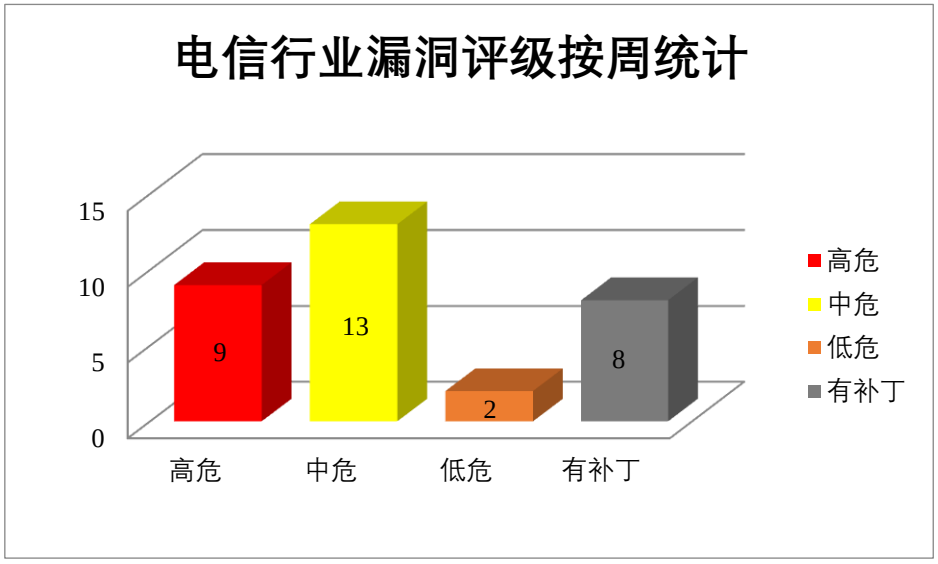

图 3 电信行业漏洞统计

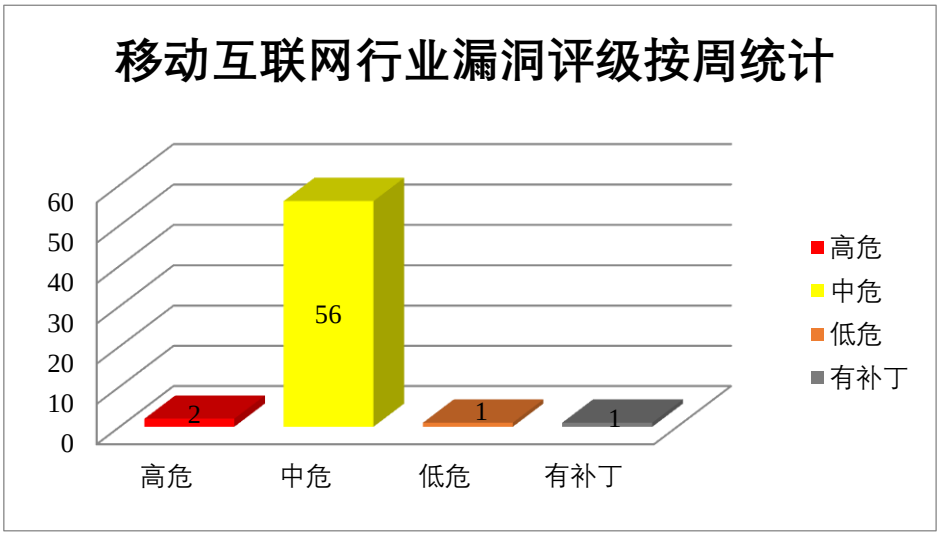

图 4 移动互联网行业漏洞统计

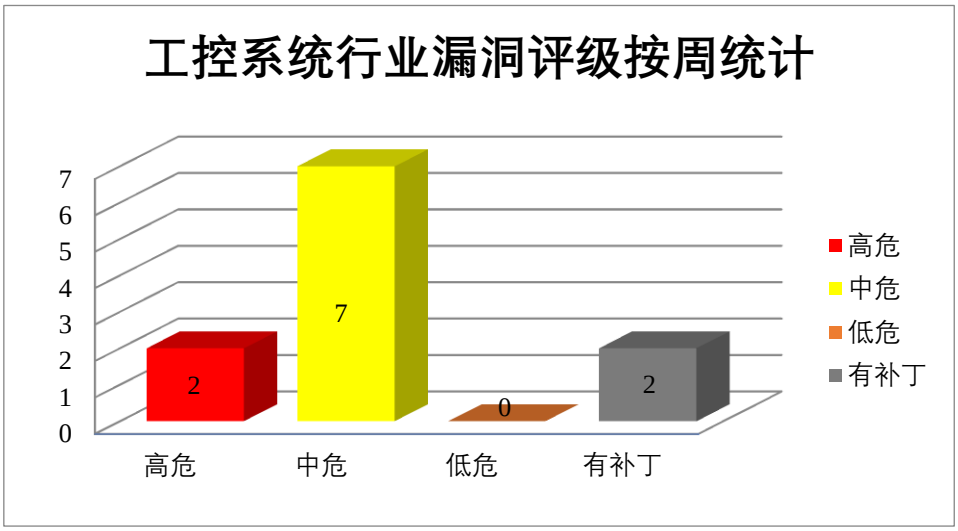

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM CICS TX Advanced 是美国国际商业机器（IBM）公司的一个事务处理监控系统，用于在企业环境中运行大规模、高事务量的应用程序。IBM Security Verify Privilege 是美国国际商业机器（IBM）公司的一个解决方案，用于管理和保护用户的身份和权限。IBM Security Guardium 是美国国际商业机器（IBM）公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Sterling Connect:Express for UNIX 是美国国际商业机器（IBM）公司的一套适用于 UNIX 平台的文件传输解决方案。IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。IBM Cognos Analytics 是美国国际商业机器（IBM）公司的一套商业智能软件。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，注入精心设计的有效载荷执行任意 Web 脚本或 HTML，通过浏览器 UI 造成拒绝服务等。

CNVD 收录的相关漏洞包括：IBM CICS TX Advanced 跨站脚本漏洞（CNVD-2024-12700）、IBM Security Verify Privilege On-Premises 信息泄露漏洞、IBM CICS TX Advanced 信息泄露漏洞、IBM Security Guardium XML 外部实体注入漏洞（CNVD-2024-12704）、IBM Sterling Connect:Express for UNIX 缓冲区溢出漏洞、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2024-12706）、IBM Cognos Analytics 访问控制错误漏洞（CNVD-2024-12708）、IBM Cognos Analytics Web UI 跨站脚本漏洞（CNVD-2024-13549）。其中，“IBM Sterling Connect:Express for UNIX 缓冲区溢出漏洞”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-2024-12700

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12702

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12701

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12704

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12703

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12706

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12708

https://www.cnvd.org.cn/flaw/show/CNVD-2024-13549

2、 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。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 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 InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。Adobe Acrobat Reader DC 是一款免费的 PDF 阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在受害者浏览器中执行恶意 JavaScript 内容，执行非授权指令，可以取得系统特权，进而进行各种非法操作，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-12462）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2024-12461）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-12465、CNVD-2024-12464、CNVD-2024-12463）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-12469）、Adobe Illustrator 资源管理错误漏洞（CNVD-2024-12467）、Adobe Acrobat Reader DC 缓冲区溢出漏洞（CNVD-2024-12466）。其中，除“Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-12462）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2024-12461）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-12469）”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-2024-12462

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12461

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12465

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12464

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12463

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12469

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12467

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12466

3、 Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致浏览器崩溃，无意中授予不打算授予的权限，使用未知的攻击向量在易受攻击的系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 拒绝服务漏洞（CNVD-2024-12547）、Mozilla Firefox 代码执行漏洞（CNVD-2024-12546、CNVD-2024-12550）、Mozilla Firefox 安全绕过漏洞（CNVD-2024-12549、CNVD-2024-12548）、Mozilla Firefox HTTP 头注入漏洞、Mozilla Firefox 越界读取漏洞（CNVD-2024-12552）、Mozilla Firefox for iOS 跨站脚本漏洞。其中，除“Mozilla Firefox for iOS 跨站脚本漏洞”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-2024-12547

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12546

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12549

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12548

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12551

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12550

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12552

https://www.cnvd.org.cn/flaw/show/CNVD-2024-12555

4、 Fortinet 产品安全漏洞

Fortinet FortiOS 是一套专用于 FortiGate 网络安全平台上的安全操作系统。Fortinet FortiProxy 是一种安全的网络代理，通过结合多种检测技术，如 Web 过滤、DNS 过滤、DLP、反病毒、入侵防御和高级威胁保护，可以保护员工免受网络攻击。Fortinet FortiPAM 是美国飞塔（Fortinet）公司的一款权限访问控制的平台。Fortinet FortiNAC 是美国飞塔（Fortinet）公司的一套网络访问控制解决方案。该产品主要用于网络访问控制和物联网安全防护。Fortinet FortiSIEM 是美国飞塔（Fortinet）公司的一套安全信息和事件管理系统。该系统包括资产发现、工作流程自动化和统一管理等功能。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃取受害者基于 cookie 的身份验证凭据，在系统上执行任意代码或命令等。

CNVD 收录的相关漏洞包括：多款 Fortinet 产品格式化字符串错误漏洞、Fortinet F

ortiOS 和 FortiProxy 空指针解引用漏洞（CNVD-2024-13019、CNVD-2024-13092）、Fortinet FortiNAC 跨站脚本漏洞（CNVD-2024-13094）、Fortinet FortiOS 和 FortiProxy 越界写入漏洞、Fortinet FortiSIEM 操作系统命令注入漏洞（CNVD-2024-13099、CNVD-2024-13100）、Fortinet FortiClientEMS CSV 注入漏洞。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-2024-13010
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13019
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13092
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13094
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13097
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13099
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13100
https://www.cnvd.org.cn/flaw/show/CNVD-2024-13532

5、PHPEMS 反序列化漏洞（CNVD-2024-13536）

PHPEMS 是一个 PHP 在线模拟考试系统。本周，PHPEMS 被披露存在反序列化漏洞。攻击者可利用该漏洞通过参数 picurl 导致反序列化。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-2024-13536

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-2024-13093	Fortinet FortiClientEMS 不适当权限管理漏洞	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://fortiguard.com/psirt/FG-IR-23-357
CNVD-2024-13527	TP-LINK ER7206 操作系统命令注入漏洞（CNVD-2024-13527）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.tp-link.com/us/support/download/er7206/v1/#Firmware
CNVD-2024-13529	TP-LINK ER7206 wireguard VPN 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.tp-link.com/us/support/download/er7206/v1/#Firmware
CNVD-2024	SAP NetWeaver 文件上传漏	高	厂商已发布了漏洞修复程序，请及

-13535	洞（CNVD-2024-13535）		时关注更新：https://me.sap.com/notes/3433192
CNVD-2024-13539	MongoDB Server 信任管理问题漏洞（CNVD-2024-13539）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://jira.mongodb.org/browse/SERVER-81312?jql=project%20%3D%20SERVER%20AND%20fixVersion%20%3D%207.1.0-rc4
CNVD-2024-13538	Moodle 拒绝服务漏洞（CNVD-2024-13538）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-74641
CNVD-2024-13541	Squid 拒绝服务漏洞（CNVD-2024-13541）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.squid-cache.org/Versions/v6/SQUID-2024_1.patch
CNVD-2024-13548	IBM MQ 输入验证错误漏洞（CNVD-2024-13548）	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/7123139
CNVD-2024-13528	TP-LINK ER7206 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复此安全问题，补丁获取链接：https://www.tp-link.com/us/support/download/er7206/v1/#Firmware
CNVD-2024-12463	Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-12463）	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/apsb24-04.html

小结：本周，IBM 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，注入精心设计的有效载荷执行任意 Web 脚本或 HTML，通过浏览器 UI 造成拒绝服务等。此外，Adobe、Mozilla、Fortinet 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在受害者浏览器中执行恶意 JavaScript 内容，执行非授权指令，可以取得系统特权，进而进行各种非法操作，在当前用户的上下文中执行任意代码等。另外，PHPEMS 被披露存在反序列化漏洞。攻击者可利用漏洞通过参数 picurl 导致反序列化。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、XunRuiCMS 跨站脚本漏洞（CNVD-2024-12713）

验证描述

XunRuiCMS（迅睿 CMS）是一套开源的内容管理系统（CMS）。

XunRuiCMS v4.6.2 及之前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向发送特制的恶意请求来获取敏感信息。

验证信息

POC 链接：https://www.cnblogs.com/rxtycc/p/17948379

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-12713

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. 舶经销商 MarineMax 遭受网络攻击

全球最大的休闲船和游艇零售商之一 MarineMax 本周透露了一次网络攻击事件，在监管文件中指出，他们于 3 月 10 日检测到一起“网络安全事件”。

参考链接：http://www.anquan419.com/knews/24/6711.html

2. Google Chrome 安全浏览保护将实时检查用户访问的网址

Google 宣布对 Chrome 浏览器的安全浏览保护功能（Safe Browsing）进行重大改变，将用户访问的网址与服务器端的恶意网站列表进行实时比对。

参考链接：https://www.solidot.org/story?sid=77602

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