国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 06 月 03 日-2024 年 06 月 09 日　　2024 年第 23 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 573 个，其中高危漏洞 308 个、中危漏洞 247 个、低危漏洞 18 个。漏洞平均分值为 6.82。本周收录的漏洞中，涉及 0day 漏洞 430 个（占 75%），其中互联网上出现“SeaCMS SQL 注入漏洞（CNVD-2024-26090）、ECshop SQL 注入漏洞（CNVD-2024-26111）”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 2293 个，与上周（4275 个）环比减少 46%。

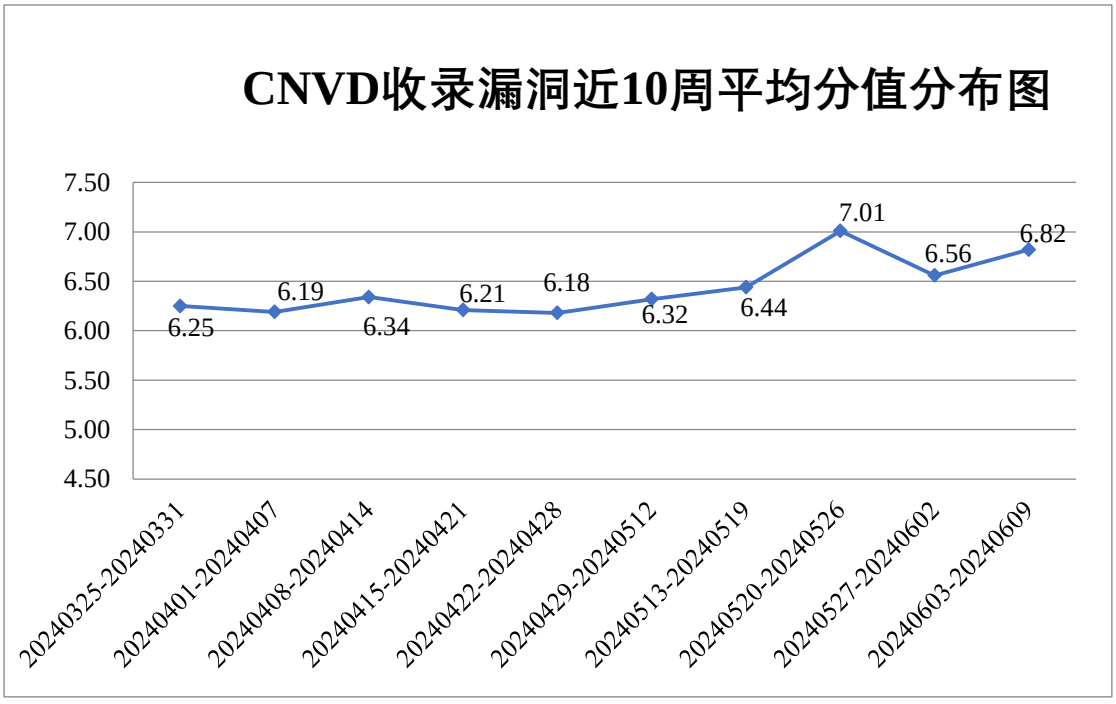

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向基础电信

企业通报漏洞事件 12 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 277 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：

紫光云技术有限公司、智互联（深圳）科技有限公司、浙江宇视科技有限公司、浙江好络维医疗技术有限公司、浙江大华技术股份有限公司、钰登科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、英飞达软件（上海）有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、西安众邦网络科技有限公司、武汉地大信息工程股份有限公司、武汉达梦数据库有限公司、万洲电气股份有限公司、天地伟业技术有限公司、索尼（中国）有限公司、苏州科达科技股份有限公司、深圳益普科技有限公司、深圳维盟网络技术有限公司、深圳市维斯易联科技有限公司、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、深圳前海华夏智信数据科技有限公司、上海熙软科技有限公司、上海穆云智能科技有限公司、上海蓝矩信息科技有限公司、上海斐讯数据通信技术有限公司、上海萃思软件有限公司、上海布雷德科技有限公司、上海博达数据通信有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山东国子软件股份有限公司、厦门印天电子科技有限公司、厦门四信通信科技有限公司、厦门科汛软件有限公司、厦门得推网络科技有限公司、融智通信息科技（天津）有限公司、麒麟软件有限公司、平凯星辰（北京）科技有限公司、鹏为软件股份有限公司、诺梵（上海）系统科技股份有限公司、南京科远智慧科技集团股份有限公司、梦想 CMS、蓝卓数字科技有限公司、科大讯飞（北京）有限公司北京软件分公司、京瓷（中国）商贸有限公司上海分公司、江苏赛达电子科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南建研信息技术股份有限公司、杭州赛脑智能科技股份有限公司、杭州平治科技有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、哈尔滨新中新电子股份有限公司、广州市和丰自动化科技有限公司、广州翰智软件有限公司、广西金中软件集团有限公司、广西海豚有海信息科技有限公司、广东飞企互联科技股份有限公司、富士胶片商业创新（中国）有限公司、福建星网锐捷通讯股份有限公司、佛山市杜特软件科技有限公司、东莞市通天星软件科技有限公司、帝国软件、创维集团有限公司、成都杰华科技有限公司、成都冠唐科技有限公司、畅捷通信息技术股份有限公司、北京中成科信科技发展有限公司、北京云标科技有限公司、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、北京心领育科技有限公司、北京微瑞集智科技有限公司、北京万户网络技术有限公司、北京天融信网络安全技术有限公司、北京神州数码云科信息技术有限公司、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、北京人大金仓信息技术股份有限公司、北京

猎鹰安全科技有限公司、北京凯特伟业科技有限公司、北京久其软件股份有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京富基融通信息技术有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京奥特美克科技股份有限公司、北京安博通科技股份有限公司、安美世纪（北京）科技有限公司、安吉加加信息技术有限公司、安徽中技国医医疗科技有限公司、安徽科迅教育装备集团有限公司、爱普生（中国）有限公司、NETGEAR、Lexmark 和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周，CNVD 发布了《F5 发布 2024 年 5 月季度安全通告》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10086）。

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、安天科技集团股份有限公司、天津市国瑞数码安全系统股份有限公司、北京数字观星科技有限公司、中国电信股份有限公司网络安全产品运营中心等单位报送公开收集的漏洞数量较多。中孚安全技术有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、北京有略安全技术有限公司、安徽天行网安信息安全技术有限公司、内蒙古洞明科技有限公司、马鞍山书拓安全科技有限公司、成都久信信息技术股份有限公司、北京中睿天下信息技术有限公司、联想集团、星云博创科技有限公司、江苏极元信息技术有限公司、中资网络信息安全科技有限公司、中国电信股份有限公司上海研究院、河南天祺信息安全技术有限公司、北京天防安全科技有限公司、北京天下信安技术有限公司、北京航空航天大学、成都安美勤信息技术股份有限公司、重庆都会信息科技有限公司、深圳昂楷科技有限公司、湖南泛联新安信息科技有限公司、联通数字科技有限公司、厦门聚丁科技有限公司、上海只柏特信息技术有限公司、上海亿保健康科技集团有限公司、广州安亿信软件科技有限公司、超聚变数字技术有限公司、江苏金盾检测技术股份有限公司、中国工商银行、中国电信股份有限公司研究院、华信咨询设计研究院有限公司、南方电网数字电网集团信息通信科技有限公司、山东云天安全技术有限公司、杭州中正检测技术有限公司及其他个人白帽子向 CNVD 提交了 2293 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）、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 655 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
新华三技术有限公司	725	0
安天科技集团股份有限公司	701	0

上海交大	446	446
天津市国瑞数码安全系统股份有限公司	393	0
北京数字观星科技有限公司	316	0
中国电信股份有限公司网络安全产品运营中心	299	299
北京天融信网络安全技术有限公司	211	7
三六零数字安全科技集团有限公司	208	208
北京神州绿盟科技有限公司	186	3
阿里云计算有限公司	163	0
华为技术有限公司	134	0
北京启明星辰信息安全技术有限公司	75	5
北京知道创宇信息技术有限公司	63	0
恒安嘉新（北京）科技股份公司	61	0
杭州安恒信息技术股份有限公司	15	0
远江盛邦（北京）网络安全科技股份有限公司	14	14
北京长亭科技有限公司	13	0
杭州迪普科技股份有限公司	11	1
京东科技信息技术有限公司	8	0
北京安信天行科技有限公司	4	4

北京智游网安科技有限公司	3	3
斗象科技（漏洞盒子）	1	1
北京升鑫网络科技有限公司（青藤云）	1	1
中孚安全技术有限公司	75	75
河南东方云盾信息技术有限公司	42	42
快页信息技术有限公司	24	24
北京有略安全技术有限公司	19	19
安徽天行网安信息安全技术有限公司	13	13
内蒙古洞明科技有限公司	12	12
马鞍山书拓安全科技有限公司	12	12
成都久信信息技术股份有限公司	10	10
北京中睿天下信息技术有限公司	6	6
联想集团	5	5
星云博创科技有限公司	4	4
江苏极元信息技术有限公司	4	4
中资网络信息安全科技有限公司	4	4
中国电信股份有限公司上海研究院	4	4
河南天祺信息安全技术有限公司	3	3
北京天防安全科技有	3	3

限公司		
北京天下信安技术有限公司	3	3
北京航空航天大学	2	2
成都安美勤信息技术股份有限公司	2	2
重庆都会信息科技有限公司	2	2
深圳昂楷科技有限公司	2	2
湖南泛联新安信息科技有限公司	2	2
联通数字科技有限公司	2	2
厦门聚丁科技有限公司	2	2
上海只柏特信息技术有限公司	1	1
上海亿保健康科技集团有限公司	1	1
广州安亿信软件科技有限公司	1	1
超聚变数字技术有限公司	1	1
江苏金盾检测技术股份有限公司	1	1
中国工商银行	1	1
中国电信股份有限公司研究院	1	1
华信咨询设计研究院有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
山东云天安全技术有	1	1

限公司		
杭州中正检测技术有限公司	1	1
CNCERT 贵州分中心	3	3
个人	1030	1030
报送总计	5352	2293

本周漏洞按类型和厂商统计

本周，CNVD 收录了 573 个漏洞。按类型划分包括 WEB 应用 324 个，应用程序 93 个，网络设备（交换机、路由器等网络端设备）79 个，智能设备（物联网终端设备）48 个，操作系统 19 个，数据库 6 个，安全产品 4。

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	324
应用程序	93
网络设备（交换机、路由器等网络端设备）	79
智能设备（物联网终端设备）	48
操作系统	19
数据库	6
安全产品	4

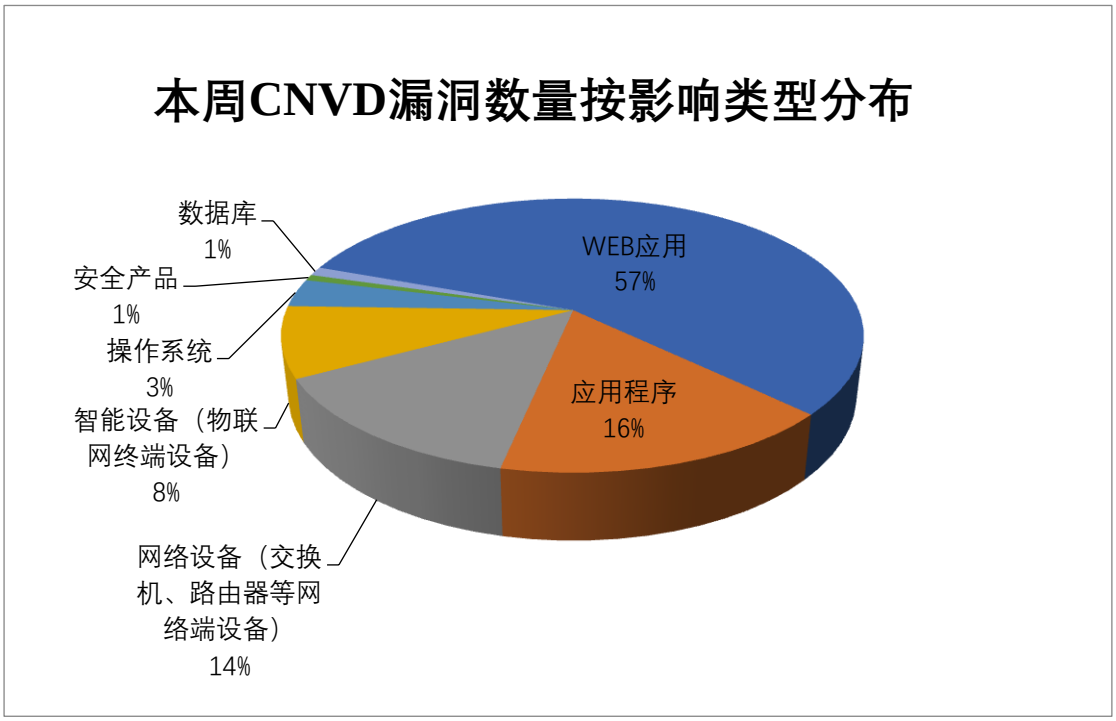

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、索尼（中国）有限公司、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	Tenda	14	3%
2	索尼（中国）有限公司	13	2%
3	Mozilla	12	2%
4	WordPress	12	2%
5	北京神州视翰科技有限公司	12	2%
6	深圳市吉祥腾达科技有限公司	12	2%
7	用友网络科技股份有限公司	11	2%
8	Microsoft	11	2%
9	Foxit	11	2%
10	其他	465	81%

本周行业漏洞收录情况

本周，CNVD 收录了 55 个电信行业漏洞，10 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“D-Link G416 代码执行漏洞、Rockwell Automation FactoryTalk View SE SQL 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/

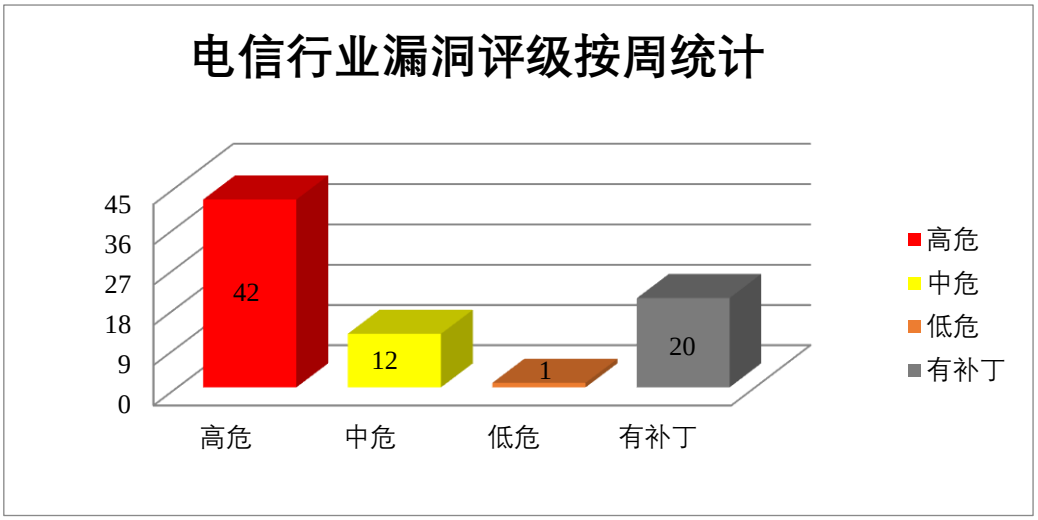

图 3 电信行业漏洞统计

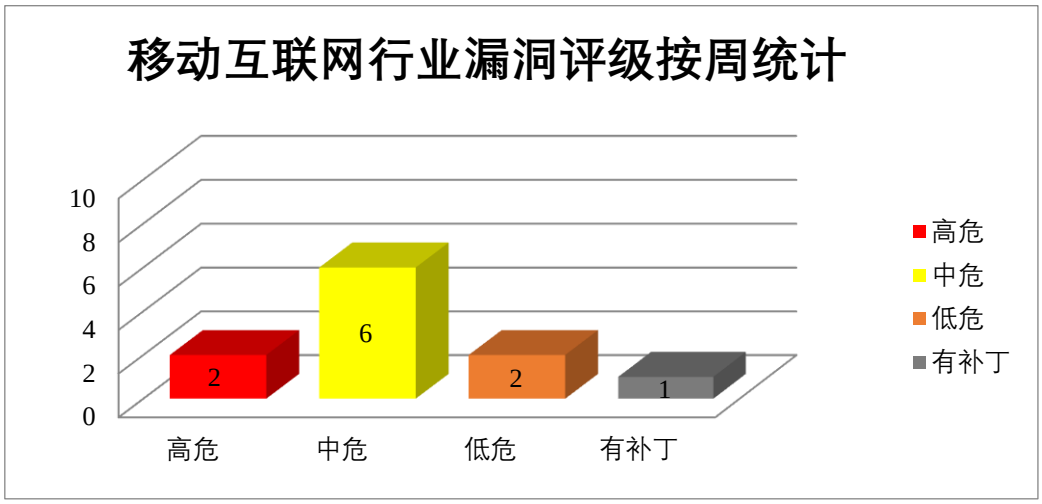

图 4 移动互联网行业漏洞统计

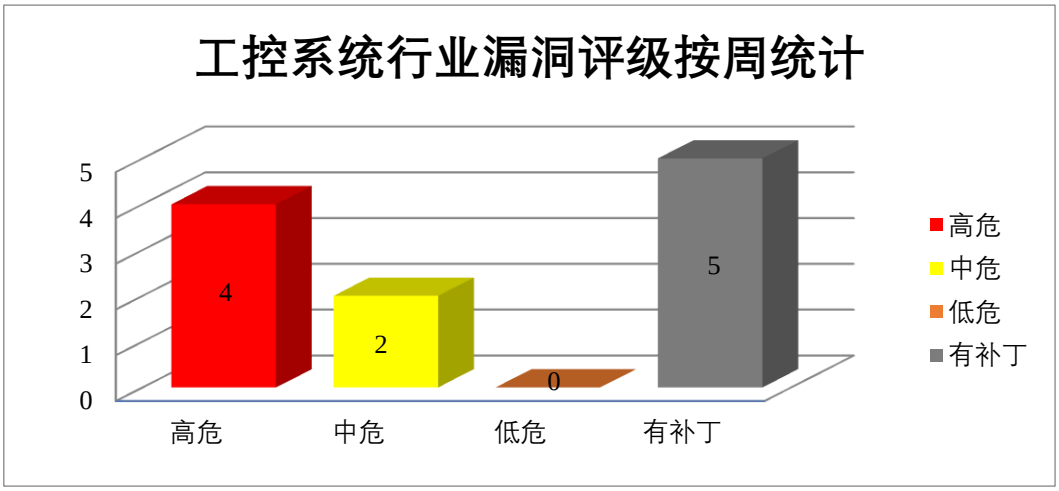

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Acrobat Reader DC 是美国奥多比（Adobe）公司的一个 Pdf 阅读工具。用于可靠查看、打印和注释 Pdf 文档。Adobe Acrobat Reader 是一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe ColdFusion 是一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。Adobe Commerce 是一种面向商家和品牌的全球领先的数字商务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的文件请求，诱使用户解析，可使应用程序崩溃或在应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 释放后使用漏洞（CNVD-2024-25606）、Adobe Acrobat Reader DC 资源管理错误漏洞（CNVD-2024-25605）、Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-25604）、Adobe ColdFusion 访问

控制错误漏洞（CNVD-2024-25609）、Adobe ColdFusion 反序列化漏洞（CNVD-2024-25608）、Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2024-25607）、Adobe Commerce 输入验证错误漏洞（CNVD-2024-25611）、Adobe Acrobat and Reader 输入验证错误漏洞（CNVD-2024-25610）。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-2024-25606
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25605
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25604
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25609
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25608
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25607
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25611
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25610

2、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：Foxit PDF Reader and Foxit PDF Editor 代码执行漏洞（CNVD-2024-25646、CNVD-2024-25645、CNVD-2024-25644、CNVD-2024-25643、CNVD-2024-25649、CNVD-2024-25648、CNVD-2024-25647、CNVD-2024-25652）。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-2024-25646
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25645
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25644
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25643
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25649
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25648
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25647
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25652

3、Mozilla 产品安全漏洞

Mozilla Focus 是美国 Mozilla 基金会的一个供 iOS 设备专用的浏览器。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。该软件支持 IMAP、POP 邮件协议以及 HTML 邮件格式。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，导致浏览器崩溃，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Focus for iOS 代码执行漏洞、Mozilla Firefox 安全绕过漏洞（CNVD-2024-25560）、Mozilla Firefox 拒绝服务漏洞（CNVD-2024-25565）、Mozilla Thunderbird 安全绕过漏洞（CNVD-2024-25572）、Mozilla Firefox 代码执行漏洞（CNVD-2024-25596）、Mozilla Firefox 和 Firefox ESR 代码执行漏洞、Mozilla Firefox for iOS 安全绕过漏洞（CNVD-2024-25612、CNVD-2024-25613）。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-2024-25490
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25560
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25565
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25572
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25596
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25602
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25612
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25613

4、Microsoft 产品安全漏洞

Microsoft OLE DB Driver for SQL Server 是独立的数据访问应用程序编程接口(API)，用于 OLE DB。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 OLE DB Driver for SQL Server 远程代码执行漏洞（CNVD-2024-25653、CNVD-2024-25656、CNVD-2024-25655、CNVD-2024-25654、CNVD-2024-25660、CNVD-2024-25659、CNVD-2024-25658、CNVD-2024-25657）。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-2024-25653
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25656
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25655
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25654
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25660
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25659
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25658
https://www.cnvd.org.cn/flaw/show/CNVD-2024-25657

5、Fortinet FortiOS 远程代码执行漏洞

Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web 内容过滤和反垃圾邮件等多种安全功能。本周，Fortinet FortiOS 被披露存在远程代码执行漏洞。攻击者可利用该漏洞远程执行代码。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-2024-26328

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-2024-25533	多款 Mozilla 产品欺骗漏洞（CNVD-2024-25533）	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/mfsa2024-05/ https://www.mozilla.org/security/advisories/mfsa2024-06/ https://www.mozilla.org/security/advisories/mfsa2024-07/
CNVD-2024-25650	Foxit PDF Reader and Foxit PDF Editor 代码执行漏洞（CNVD-2024-25650）	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
CNVD-2024-25661	Microsoft OLE DB Driver for SQL Server 远程代码执行漏洞（CNVD-2024-25661）	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-2024-29983
CNVD-2024-26019	Mitsubishi Electric MELSEC-Q Series 和 MELSEC-L Series 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf
CNVD-2024-26045	Rockwell Automation ControlLogix and GuardLogix 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://www.rockwellautomation.com/en-us.html
CNVD-2024-26081	Dell Data Protection Advisor 加密问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000225088/dsa-2024-192-secur

			ity-update-for-data-protection-advisor-and-powerprotect-dp-series-appliance-idpa-for-multiple-vulnerabilities
CNVD-2024-26094	Ivanti EPM SQL 注入漏洞（CNVD-2024-26094）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
CNVD-2024-26095	Ivanti EPM SQL 注入漏洞（CNVD-2024-26095）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://forums.ivanti.com/s/article/Security-Advisory-May-2024
CNVD-2024-26187	Apache OFBiz 路径遍历漏洞（CNVD-2024-26187）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ofbiz.apache.org/download.html
CNVD-2024-26330	Tenda W15E formQOSRuleDel 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-2722.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交特殊的文件请求，诱使用户解析，可使应用程序崩溃或在应用程序上下文执行任意代码等。此外，Foxit、Mozilla、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，导致浏览器崩溃，在系统上执行任意代码等。另外，Fortinet FortiOS 被披露存在远程代码执行漏洞。攻击者可利用漏洞远程执行代码。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、ECShop SQL 注入漏洞（CNVD-2024-26111）

验证描述

ShopeX ECShop 是中国商派（ShopeX）公司的一个开源商城系统。支持 PC+H5+APP+小程序商城，源码免费下载体验，适合企业开发搭建商城。

ECShop 存在 SQL 注入漏洞，该漏洞源于 file/article.php 组件缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞查看、添加、修改或删除后端数据库中的信息。

验证信息

POC 链接：https://github.com/mortal-sec/CVE-2024-31025

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-26111

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. Zyxel 发布针对 EoL NAS 型号固件漏洞的补丁

Zyxel 发布了安全更新，以解决影响其两台网络连接存储（NAS）设备的关键缺陷，这些设备目前已达到生命周期终止（EoL）状态。

参考链接：https://thehackernews.com/2024/06/zyxel-releases-patches-for-firmware.html

2. Cox Biz 自动绕过漏洞导致信息泄露

如果漏洞被利用，攻击者不仅可以获取企业客户的个人身份信息（PII），还可以获取 Wi-Fi 密码和连接设备上的信息，甚至可能在设备上执行任意要求、更新设备或接管客户账户。

参考链接：https://www.darkreading.com/application-security/cox-biz-auth-bypass-bug-millions-devices-takeover

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