国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 09 月 30 日-2024 年 10 月 13 日 **2024 年第 40、41 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 378 个，其中高危漏洞 232 个、中危漏洞 126 个、低危漏洞 20 个。漏洞平均分值为 6.88。本周收录的漏洞中，涉及 0day 漏洞 219 个（占 58%），其中互联网上出现“Tenda AX 1806 serverName 参数堆栈溢出漏洞、Tenda AX1806 iptv.stb.port 参数堆栈溢出漏洞”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 9281 个，与上周（8664 个）环比增加 7%。

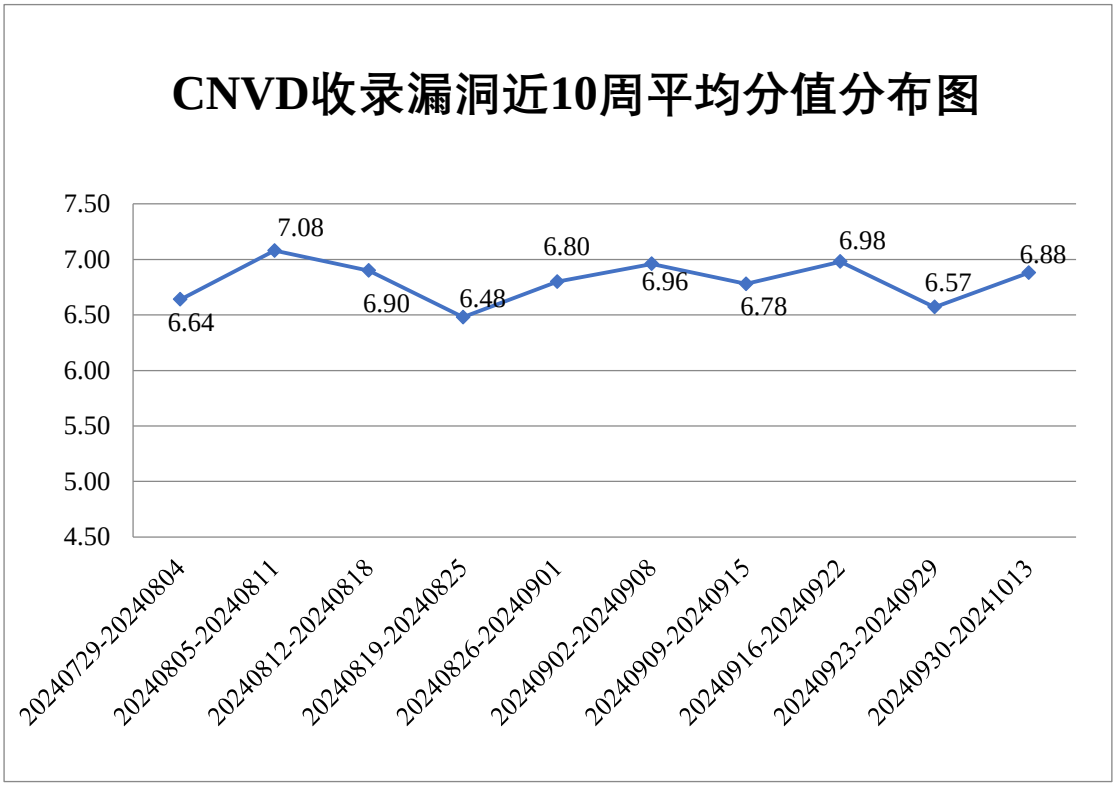

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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，CNVD 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 596 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 19 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：

方天科技（深圳）有限公司、紫光软件系统有限公司、重庆紫光华山智安科技有限公司、重庆金鑫科技产业发展有限公司、中科数字通（北京）科技有限公司、郑州微笑智能科技有限公司、郑州金鼓通信技术有限公司、浙江宇视科技有限公司、浙江快服集团有限公司、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、长沙友点软件科技有限公司、云南链滴科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、徐州亿优网架钢结构工程有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新晨科技股份有限公司、校无忧科技网络公司、无锡信捷电气股份有限公司、网域数据安全(深圳)有限公司、砼联数字科技有限公司、天津市国瑞数码安全系统股份有限公司、天津南大通用数据技术股份有限公司、石家庄市征红网络科技有限公司、石家庄和嘉科技有限公司、深圳维盟网络技术有限公司、深圳市中科网威科技有限公司、深圳市云盟智慧科技有限公司、深圳市亿玛信诺科技有限公司、深圳市鑫塔科技有限公司、深圳市唯德科创信息有限公司、深圳市思迅软件股份有限公司、深圳市玛威尔显控科技有限公司、深圳市龙信信息技术有限公司、深圳市联天通信技术有限公司、深圳市利谱信息技术有限公司、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、深圳市和为顺网络技术有限公司、深圳市必联电子有限公司、深圳彼度科技有限公司、深圳奥联信息安全技术有限公司、上海卓卓网络科技有限公司、上海灵当信息科技有限公司、上海戴德网络科技有限公司、上海冰峰计算机网络技术有限公司、上海艾泰科技有限公司、陕西时光软件有限公司、山东思达特测控设备有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、山东比特智能科技股份有限公司、厦门四信通信科技有限公司、瑞斯康达科技发展股份有限公司、曲靖蜂信科技有限公司、青果软件集团有限公司、麒麟软件有限公司、南京星远图科技有限公司、罗格朗（上海）管理有限公司、联奕科技股份有限公司、廊坊市极致网络科技有限公司、柯尼卡美能达（中国）投资有限公司、玖峰管理咨询有限公司、京瓷办公信息系统（中国）有限公司、江西铭软科技有限公司、江苏浪潮信息咨询有限公司、惠普贸易（上海）有限公司、华平信息技术股份有限公司、湖南中彩科技有限公司、河南新天软件技术有限公司、河南大华安防科技股份有限公司、合肥六出网络科技有限公司、贵州宏信创达工程检测咨询有限公

司、广州同聚成电子科技有限公司、广州市保伦电子有限公司、广州巨杉软件开发有限公司、广州红海云计算股份有限公司、广西南宁领众网络科技有限公司、广联达科技股份有限公司、广东卓锐软件有限公司、广东顺景软件科技有限公司、广东世纪信通科技股份有限公司、广东保伦电子股份有限公司、甘肃文旅产业集团有限公司、福建顶点软件股份有限公司、敦陽科技股份有限公司、东芝（中国）有限公司、大庆紫金桥软件技术有限公司、大连华天软件有限公司、成都零起飞科技有限公司、畅捷通信息技术股份有限公司、北京中科网威信息技术有限公司、北京中教启星科技股份有限公司、北京优锘科技有限公司、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、北京西斯耐特自动化技术有限公司、北京威努特技术有限公司、北京万户网络技术有限公司、北京胜能能源科技有限公司、北京神州视翰科技有限公司、北京三维天地科技股份有限公司、北京人大金仓信息技术股份有限公司、北京美特软件技术有限公司、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、北京国炬信息技术有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司和阿里巴巴集团安全应急响应中心。

本周，CNVD 发布了《Microsoft 发布 2024 年 10 月安全更新》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10486）。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、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、北京神州绿盟科技有限公司、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。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、江苏金盾检测技术股份有限公司、快页信息技术有限公司、淮安易云科技有限公司、北京翰慧投资咨询有限公司、河南灵创电子科技有限公司、星云博创科技有限公司、北京卓识网安技术股份有限公司、江苏云天网络安全技术有限公司、北京大学、联通数字科技有限公司、信息产业信息安全测评中心、中资网络信息安全科技有限公司、上海观安信息技术股份有限公司、安徽天行网安信息安全技术有限公司、贵州多彩网安科技有限公司、江苏正信信息安全测试有限公司、吉林省吉林祥云信息技术有限公司、北京航空航天大学、苏州棱镜七彩信息科技有限公司、广东粤密技术服务有限公司、星舟有信（北京）信息技术有限公司、北京天下信安技术有限公司、上海维信荟智金融科技有限公司、北京山石网科信息技术有限公司、四川电科宏安科技有限公司、中能融合智慧科技有限公司、杭州默安科技有限公司、平安银河实验室、成都久信信息技术股份有限公司、中电云数智科技有限公司、北京时代新威信息技术有限公司、亚信科技（成都）有限公司、南方电网科学研究院有限责任公司、中华人民共和国上海海事局、江苏极元信息技术有限公司、中电万维信息技术有限责任公

司、上海市信息安全测评认证中心、西安交大捷普网络科技有限公司、浙江木链物联网科技有限公司及其他个人白帽子向 CNVD 提交了 9281 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 7040 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）	4440	4440
深信服科技股份有限公司	3304	25
三六零数字安全科技集团有限公司	1461	1461
上海交大	1139	1139
北京启明星辰信息安全技术有限公司	917	9
新华三技术有限公司	824	0
北京神州绿盟科技有限公司	794	88
北京天融信网络安全技术有限公司	657	12
杭州安恒信息技术股份有限公司	183	159
阿里云计算有限公司	165	2
北京升鑫网络科技有限公司（青藤云）	110	110
恒安嘉新（北京）科技股份公司	103	0
华为技术有限公司	81	1
北京知道创宇信息技术有限公司	36	4
远江盛邦（北京）网络安全科技股份有限公司	32	32
北京数字观星科技有限公司	29	0
北京长亭科技有限公	19	5

司		
奇安信网神（补天平台）	10	10
南京众智维信息科技有限公司	6	6
长春嘉诚信息技术股份有限公司	2	2
北京智游网安科技有限公司	1	1
成都卫士通信息安全技术有限公司	216	216
河南东方云盾信息技术有限公司	45	45
江苏金盾检测技术股份有限公司	34	34
快页信息技术有限公司	29	29
西门子（中国）有限公司	28	0
淮安易云科技有限公司	17	17
北京翰慧投资咨询有限公司	16	16
河南灵创电子科技有限公司	15	15
星云博创科技有限公司	13	13
北京卓识网安技术股份有限公司	12	12
江苏云天网络安全技术有限公司	10	10
北京大学	10	10
联通数字科技有限公司	8	8
信息产业信息安全测	6	6

评中心		
中资网络信息安全科技有限公司	5	5
上海观安信息技术股份有限公司	5	5
安徽天行网安信息安全技术有限公司	4	4
贵州多彩网安科技有限公司	3	3
江苏正信信息安全测试有限公司	3	3
吉林省吉林祥云信息技术有限公司	3	3
北京航空航天大学	3	3
苏州棱镜七彩信息科技有限公司	3	3
广东粤密技术服务有限公司	3	3
星舟有信（北京）信息技术有限公司	3	3
北京天下信安技术有限公司	2	2
上海维信荟智金融科技有限公司	2	2
北京山石网科信息技术有限公司	2	2
四川电科宏安科技有限公司	2	2
中能融合智慧科技有限公司	2	2
杭州默安科技有限公司	2	2
平安银河实验室	2	2
成都久信信息技术股份有限公司	1	1

中电云数智科技有限公司	1	1
北京时代新威信息技术有限公司	1	1
亚信科技（成都）有限公司	1	1
南方电网科学研究院有限责任公司	1	1
中华人民共和国上海海事局	1	1
江苏极元信息技术有限公司	1	1
中电万维信息技术有限责任公司	1	1
上海市信息安全测评认证中心	1	1
西安交大捷普网络科技有限公司	1	1
浙江木链物联网科技有限公司	1	1
CNCERT 宁夏分中心	21	21
CNCERT 内蒙古分中心	1	1
CNCERT 贵州分中心	1	1
个人	1261	1261
报送总计	16116	9281

本周漏洞按类型和厂商统计

本周，CNVD 收录了 378 个漏洞。WEB 应用 128 个，应用程序 109 个，网络设备（交换机、路由器等网络端设备）89 个，操作系统 29 个，智能设备（物联网终端设备）14 个，安全产品 5 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	128
应用程序	109

网络设备（交换机、路由器等网络端设备）	89
操作系统	29
智能设备（物联网终端设备）	14
安全产品	5
数据库	4

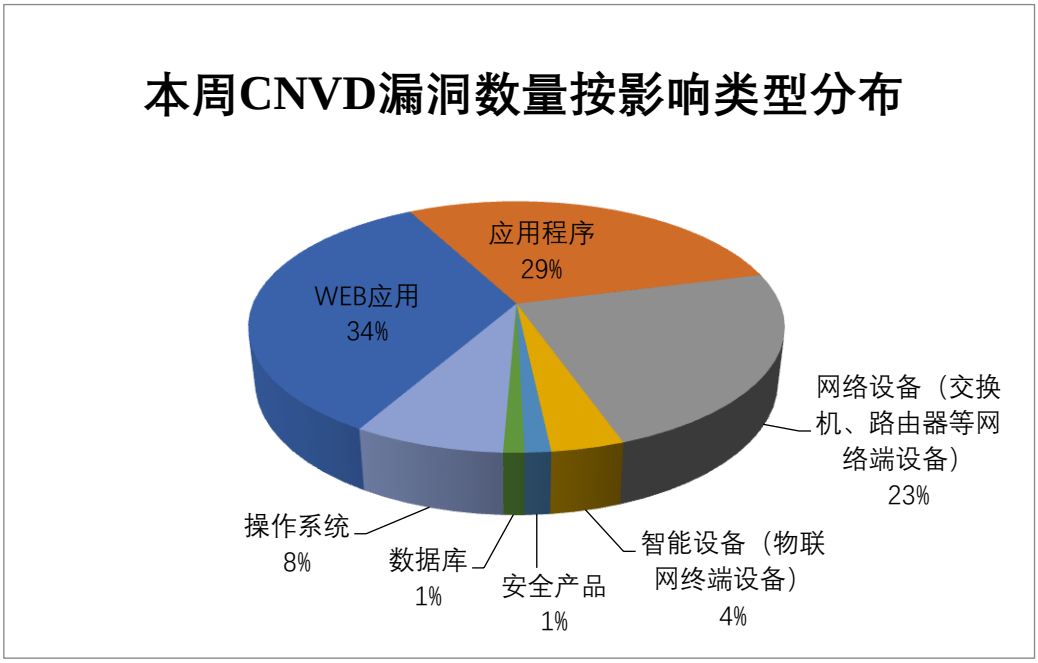

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Tenda、Google 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	Siemens	28	7%
2	Tenda	20	5%
3	Google	19	5%
4	Linux	18	5%
5	Adobe	17	5%
6	Microsoft	16	4%
7	DrayTek	15	4%
8	Mozilla	14	4%
9	Vim	12	3%
10	其他	219	58%

本周行业漏洞收录情况

本周，CNVD 收录了 59 个电信行业漏洞，16 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，“Google Android 权限提升漏洞（CNVD-2024-39681）、DrayTek Vigor 3910 缓冲区溢出漏洞”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/

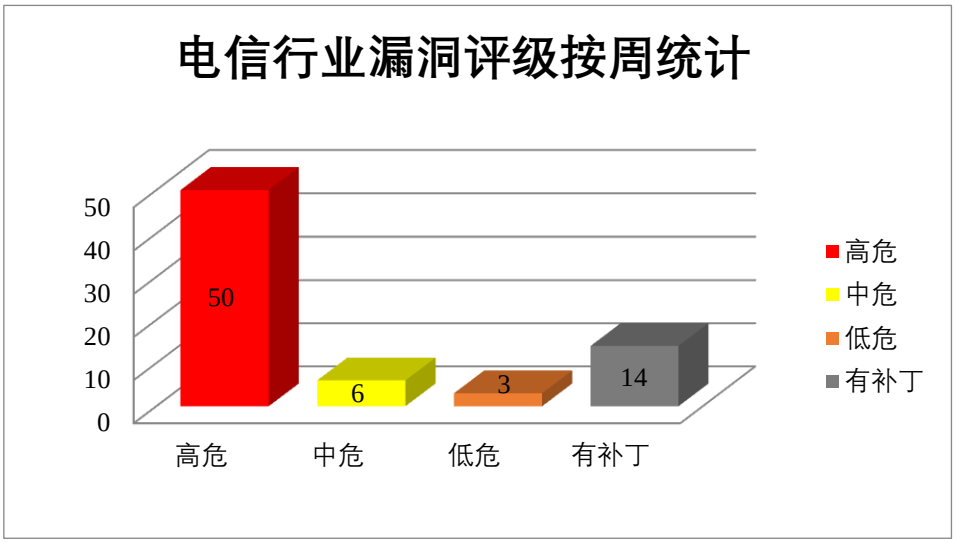

图 3 电信行业漏洞统计

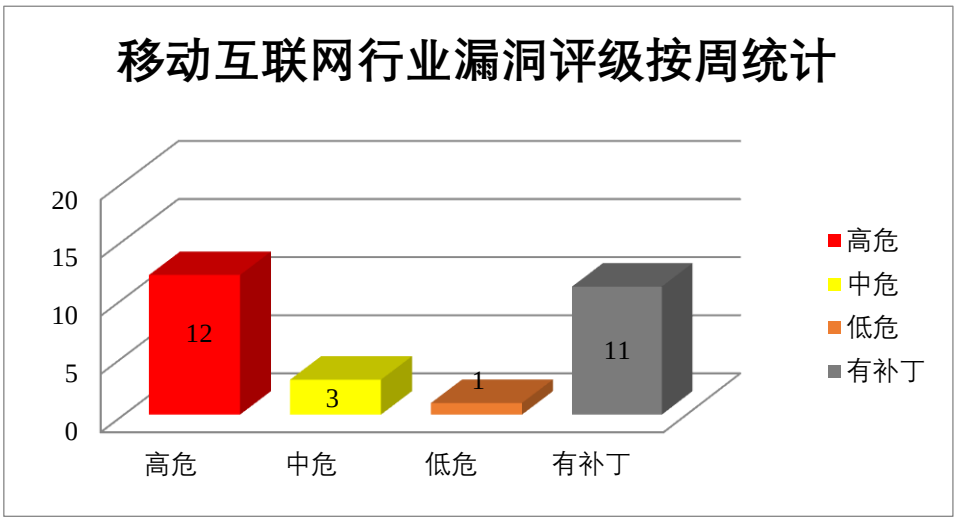

图 4 移动互联网行业漏洞统计

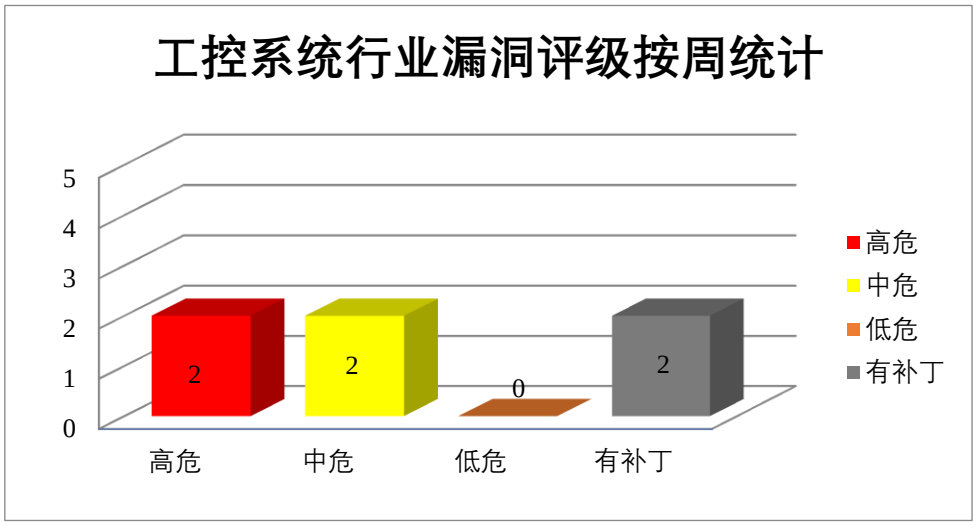

图 5 工控系统行业漏洞统计

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、 Mozilla 产品安全漏洞

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。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品信息泄露漏洞（CNVD-2024-40518）、多款 Mozilla 产品代码执行漏洞（CNVD-2024-40520、CNVD-2024-40521、CNVD-2024-40522、CNVD-2024-40525、CNVD-2024-40524）、Mozilla Firefox 和 Firefox ESR 安全绕过漏洞（CNVD-2024-40519）、Mozilla Firefox 代码执行漏洞（CNVD-2024-40523）。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-2024-40518

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40520

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40519

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40521

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40523

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40522

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40525

https://www.cnvd.org.cn/flaw/show/CNVD-2024-40524

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 SharePoint Server 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。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，获取敏感信息，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge (Chromium-based)信息泄露漏洞（CNVD-2024-39657）、Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-39656）、Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-39671、CNVD-2024-39672、CNVD-2024-39674、CNVD-2024-39677）、Microsoft SharePoint Server 信息泄露漏洞（CNVD-2024-39673）、Microsoft SharePoint Server 欺骗漏洞（CNVD-2024-39676）。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-2024-39657
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39656
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39671
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39672
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39673
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39674
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39676
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39677

3、 Adobe 产品安全漏洞

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe InCopy 是美国奥多比（Adobe）公司的一款用于创作的文本编辑软件。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 Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Substance 3D Stager 是美国奥多比（Adobe）公司的一个虚拟 3D 工作室。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。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。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，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Adobe Photoshop 资源管理错误漏洞（CNVD-2024-39915）、Adobe InCopy 输入验证错误漏洞（CNVD-2024-39914）、Adobe Illustrator 拒绝服务漏洞（CNVD-2024-39913）、Adobe Commerce 身份验证错误漏洞（CNVD-2024-39912）、Adobe Substance 3D Stager 资源管理错误漏洞（CNVD-2024-39916）、Adobe Acrobat and Reader 代码执行漏洞（CNVD-2024-39920）、Adobe Acrobat Reader

缓冲区溢出漏洞（CNVD-2024-39919、CNVD-2024-39918）。其中，除“Adobe Illustrator 拒绝服务漏洞（CNVD-2024-39913）”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-2024-39915
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39914
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39913
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39912
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39916
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39920
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39919
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39918

4、Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上获得更高的权限，执行任意代码，或者导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2024-39682、CNVD-2024-39683、CNVD-2024-39684、CNVD-2024-39686、CNVD-2024-39688）、Google Chrome 安全绕过漏洞（CNVD-2024-39738）、Google Chrome 代码执行漏洞（CNVD-2024-39741）、Google Chrome 缓冲区溢出漏洞（CNVD-2024-39746）。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-2024-39682
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39683
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39684
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39686
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39688
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39738
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39741
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39746

5、TOTOLINK X5000R ipsecL2tpEnable 参数代码执行漏洞

TOTOLINK X5000R 是中国吉翁电子（TOTOLINK）公司的一个路由器。本周，TOTOLINK X5000R 被披露存在代码执行漏洞。攻击者可利用该漏洞执行任意代码。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-2024-40408

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-2024-40023	Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2024-40023）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sw.siemens.com/product/297028302/ https://support.sw.siemens.com/product/297028302/
CNVD-2024-39666	GTKWave 操作系统命令注入漏洞（CNVD-2024-39666）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/
CNVD-2024-39679	Advantech ADAM-5550 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/
CNVD-2024-39943	DrayTek Vigor 3910 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.draytek.com/products/vigor3910/
CNVD-2024-40009	Siemens Simcenter Nastran 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sw.siemens.com/
CNVD-2024-40471	Vim 代码执行漏洞（CNVD-2024-40471）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim/commit/816fbcc262687b81fc46f82f7bbeb1453addfe0c
CNVD-2024-39668	GTKWave 操作系统命令注入漏洞（CNVD-2024-39668）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/
CNVD-2024-39680	Advantech ADAM-5630 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/
CNVD-2024-39951	DrayTek Vigor 3910 缓冲区溢出漏洞（CNVD-2024-39951）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.draytek.com/products/vigor3910/
CNVD-2024	Siemens JT2Go 堆栈缓冲区	高	厂商已发布了漏洞修复程序，请及

-40011	溢出漏洞		时关注更新：https://plm.sw.siemens.com/en-US/plm-components/jt/jt2go/

小结：本周，Mozilla 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，获取敏感信息，执行任意代码或造成拒绝服务。此外，Microsoft、Adobe、Google 等多款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，在系统上获得更高的权限，获取敏感信息，执行任意代码，导致拒绝服务等。另外，TOTOLINK X5000R 被披露存在代码执行漏洞。攻击者可利用该漏洞执行任意代码。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、Tenda AX1806 serverName 参数堆栈溢出漏洞

验证描述

Tenda AX1806 是中国腾达（Tenda）公司的一个 WiFi6 无线路由器。

Tenda AX1806 serverName 参数存在堆栈溢出漏洞，该漏洞源于 form_fast_setting_internet_set 方法的 serverName 参数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。

验证信息

POC 链接：https://detailed-stetson-767.notion.site/Tenda-AX1806-Buffer-Overflow-in-form_fast_setting_internet_set-fe072267132d42be935ea4d7a53f7369

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-40416

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. GitLab 曝出安全漏洞，可能导致任意 CI/CD 管道执行

近日，GitLab 发布了社区版（CE）和企业版（EE）的安全更新，以解决八个安全漏洞，其中包括一个可能允许在任意分支上运行持续集成和持续交付（CI/CD）管道的安全漏洞。该漏洞被跟踪为 CVE-2024-9164，CVSS 得分为 9.6（满分 10 分），攻击者可以在某些情况下以任意用户身份触发 Pipeline，可能导致权限提升或执行恶意操作。

参考链接：https://www.freebuf.com/news/412651.html

2. 研究人员在 Windows 版的 SVN 中发现代码执行漏洞

Apache Subversion（SVN）是一款广受开发者欢迎的版本控制系统，用于维护源代码、网页和文档。最近，Apache Subversion 中发现了一个安全漏洞，CVE-2024-45720（CVSS 评分 8.2）。该漏洞主要影响 Windows 平台，可能导致命令行参数注入，从而执行非预期的程序。

参考链接：https://www.freebuf.com/news/412549.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