国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 08 月 05 日-2024 年 08 月 11 日 **2024 年第 32 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**高**。

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 217 个，其中高危漏洞 117 个、中危漏洞 95 个、低危漏洞 5 个。漏洞平均分值为 7.08。本周收录的漏洞中，涉及 0day 漏洞 109 个（占 50%），其中互联网上出现“AJ-Report SQL 注入漏洞（CNVD-2024-34975）、福州网钛软件科技有限公司 idcCMS 跨站请求伪造漏洞”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 26411 个，与上周（45205 个）环比减少 42%。

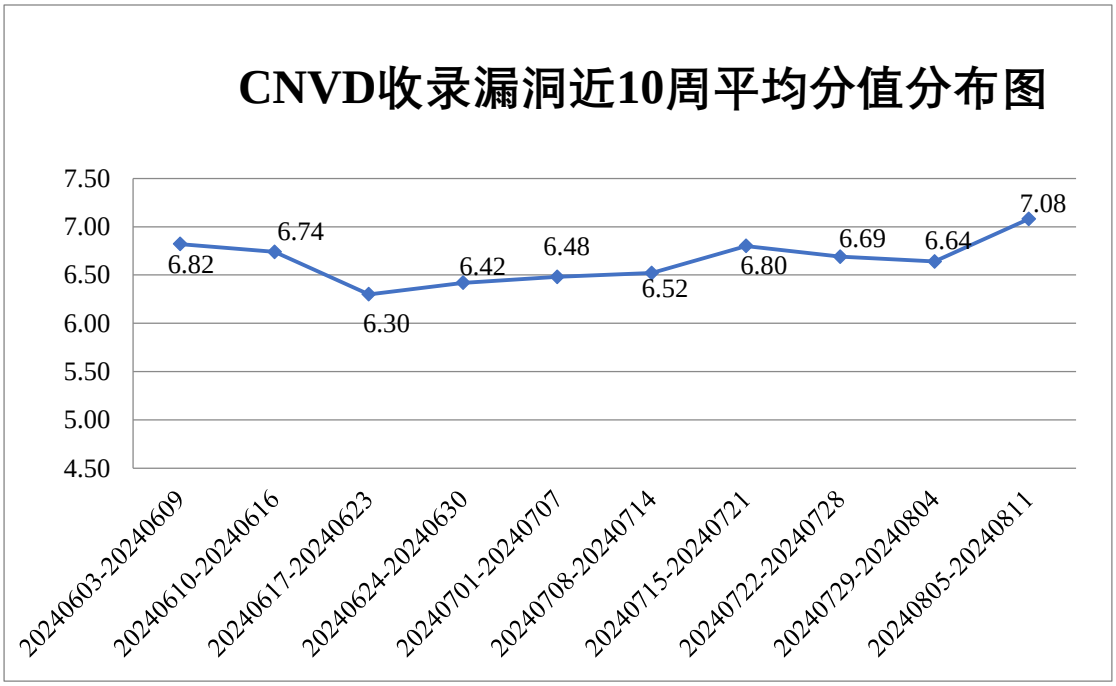

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向基础电信

企业通报漏洞事件 2 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 360 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 37 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 14 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、珠海市安克电子技术有限公司、中建材信息技术股份有限公司、正奇晟业（北京）科技有限公司、浙江宇视科技有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、长沙德尚网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、雅马哈乐器音响（中国）投资有限公司、无锡开云信息技术有限公司、广州图创计算机软件开发有限公司、天津神州浩天科技有限公司、四川迅睿云软件开发有限公司、神州数码控股有限公司、深圳市四海众联网络科技有限公司、深圳市锐明技术股份有限公司、深圳市必联电子有限公司、深圳海威达科技有限公司、上海卓卓网络科技有限公司、上海甄云信息科技有限公司、上海三高计算机中心股份有限公司、上海泛微网络科技股份有限公司、山西汽运集团云易网络科技有限公司、山石网科通信技术（北京）有限公司、山东金钟科技集团股份有限公司、山东德尔智能数码股份有限公司、厦门纳龙健康科技股份有限公司、厦门科拓通讯技术股份有限公司、青岛三利集团有限公司、青岛和正信息技术有限公司、麒麟软件有限公司、普联技术有限公司、南京南瑞信通科技有限公司、金蝶国际软件集团有限公司、江阴汇智软件技术有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、恒信汽车集团股份有限公司、杭州新中大科技股份有限公司、杭州千宜科技有限公司、杭州荷花软件有限公司、哈尔滨新中新电子股份有限公司、贵阳思普信息技术有限公司、广州易凯软件技术有限公司、广州市玄武无线科技股份有限公司、广州恒企教育科技有限公司、广东飞企互联科技股份有限公司、福建远控科技有限公司、福建博思软件股份有限公司、飞救医疗科技（北京）有限公司、东莞市通天星软件科技有限公司、东方网力科技股份有限公司、东北师大理想软件股份有限公司、成都同飞科技有限责任公司、成都天问互联科技有限公司、成都索贝数码科技股份有限公司、成都光大网络科技有限公司、畅捷通信息技术股份有限公司、博锐尚格科技股份有限公司、北京中创视讯科技有限公司、北京炎黄盈动科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京万向新元科技股份有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京软虹科技有限公司、北京金和网络股份有限公司、北京海量数据技术股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安徽新中新华科电子有限公司、安徽科迅教育装备集团有限公司和安徽九广全景智慧科技有限公司。

本周，CNVD 发布了《关于 Windows 远程桌面许可服务存在远程代码执行漏洞的安全公告》和《亿赛通公司发布电子文档安全管理系统产品补丁更新》。详情参见 CNVD

网站公告内容。

https://www.cnvd.org.cn/webinfo/show/10286

https://www.cnvd.org.cn/webinfo/show/10291

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、北京天融信网络安全技术有限公司、新华三技术有限公司、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、快页信息技术有限公司、河南东方云盾信息技术有限公司、重庆都会信息科技有限公司、北京翰慧投资咨询有限公司、江苏锋刃信息科技有限公司、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、江苏云天网络安全技术有限公司、中资网络信息安全科技有限公司、江苏晟晖信息科技有限公司、甘肃赛飞安全科技有限公司、河南天祺信息安全技术有限公司、国家体育总局体育彩票管理中心、成都久信信息技术股份有限公司、广州万方计算机科技有限公司、北京天下信安技术有限公司、北京亿赛通科技发展有限责任公司、厦门聚丁科技有限公司、马鞍山书拓安全科技有限公司及其他个人白帽子向 CNVD 提交了 26411 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）、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 25351 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
奇安信网神（补天平台）	21547	21547
斗象科技（漏洞盒子）	3097	3097
深信服科技股份有限公司	727	11
北京天融信网络安全技术有限公司	445	6
新华三技术有限公司	408	0
三六零数字安全科技集团有限公司	363	363
上海交大	344	344
安天科技集团股份有限公司	302	0
阿里云计算有限公司	165	0

恒安嘉新（北京）科技股份公司	98	0
北京启明星辰信息安全技术有限公司	81	14
杭州安恒信息技术股份有限公司	69	42
北京知道创宇信息技术有限公司	31	4
北京长亭科技有限公司	18	3
中国电信集团系统集成有限责任公司	15	15
远江盛邦（北京）网络安全科技股份有限公司	14	14
长春嘉诚信息技术股份有限公司	7	7
北京安信天行科技有限公司	7	7
江苏金盾检测技术股份有限公司	39	39
快页信息技术有限公司	36	36
河南东方云盾信息技术有限公司	22	22
重庆都会信息科技有限公司	13	13
北京翰慧投资咨询有限公司	10	10
江苏锋刃信息科技有限公司	9	9
北京山石网科信息技术有限公司	7	7
江苏正信信息安全测试有限公司	6	6

江苏云天网络安全技术有限公司	4	4
中资网络信息安全科技有限公司	3	3
江苏晟晖信息科技有限公司	3	3
甘肃赛飞安全科技有限公司	2	2
河南天祺信息安全技术有限公司	2	2
国家体育总局体育彩票管理中心	1	1
成都久信信息技术股份有限公司	1	1
广州万方计算机科技有限公司	1	1
北京天下信安技术有限公司	1	1
北京亿赛通科技发展有限责任公司	1	1
厦门聚丁科技有限公司	1	1
马鞍山书拓安全科技有限公司	1	1
CNCERT 贵州分中心	1	1
CNCERT 福建分中心	1	1
个人	772	772
报送总计	28675	26411

本周漏洞按类型和厂商统计

本周，CNVD 收录了 217 个漏洞。WEB 应用 87 个，应用程序 55 个，数据库 29 个，网络设备（交换机、路由器等网络端设备）28 个，智能设备（物联网终端设备）13 个，操作系统 5 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	87
应用程序	55
数据库	29
网络设备（交换机、路由器等网络端设备）	28
智能设备（物联网终端设备）	13
操作系统	5

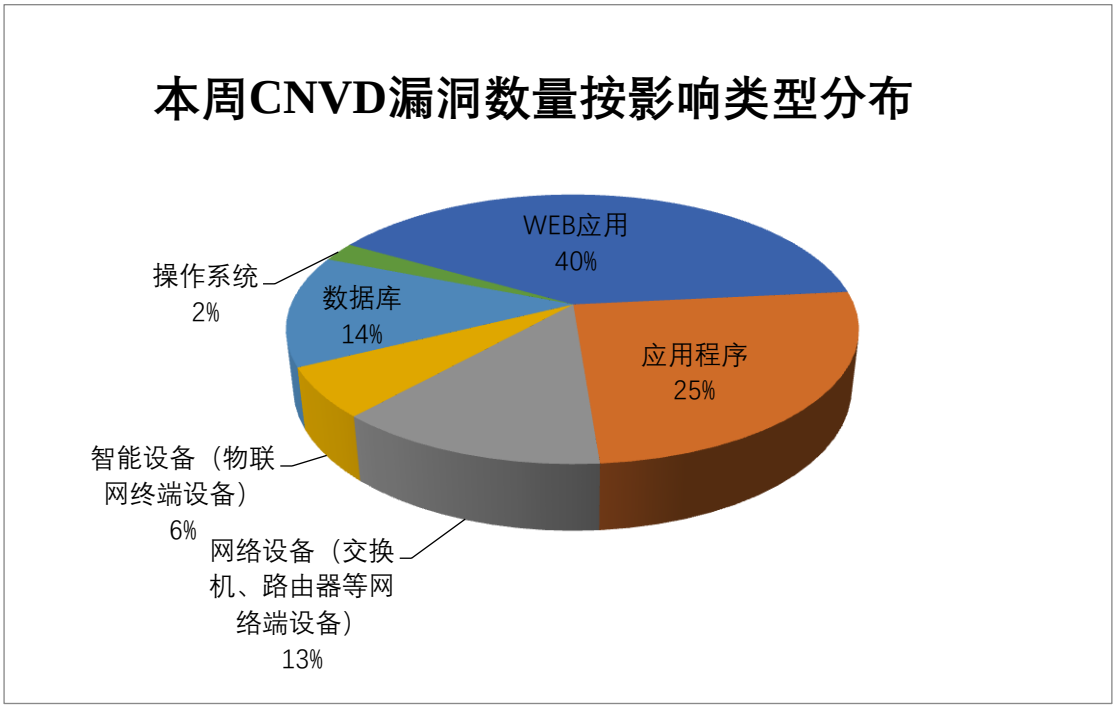

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Solarwinds 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	Oracle	24	11%
2	Google	18	8%
3	Solarwinds	12	6%
4	Dell	11	5%
5	Mozilla	10	5%
6	Adobe	10	5%
7	杭州雄伟科技开发股份有限公司	6	3%
8	ASUS	6	3%
9	用友网络科技股份有限公司	5	2%

10	其他	115	52%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，2 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation Pavilion 8 权限提升漏洞、AutomationDirect P3-550E 越界写入漏洞”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/

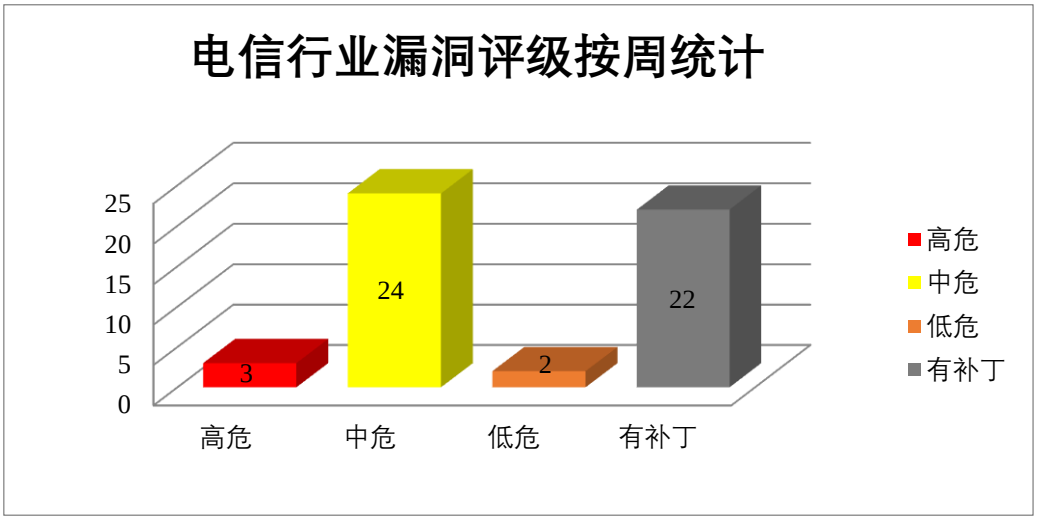

图 3 电信行业漏洞统计

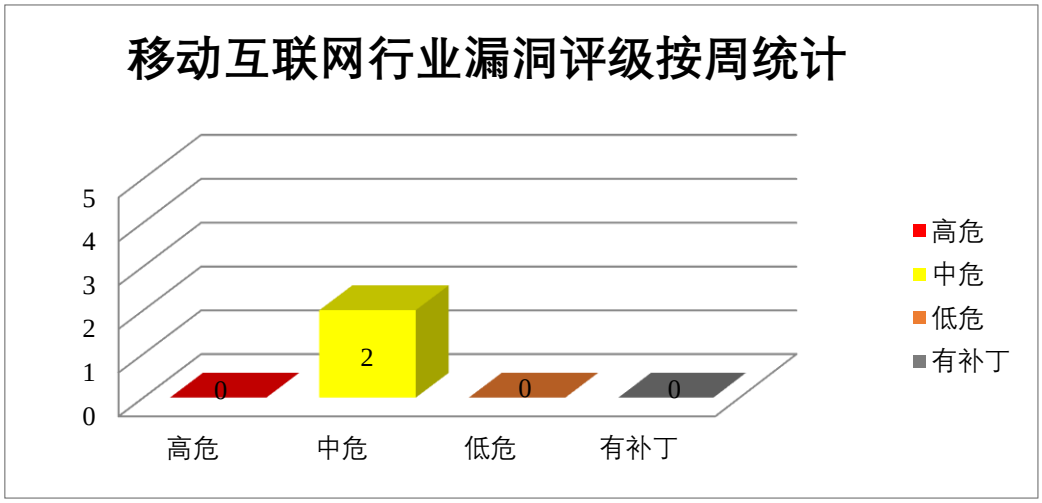

图 4 移动互联网行业漏洞统计

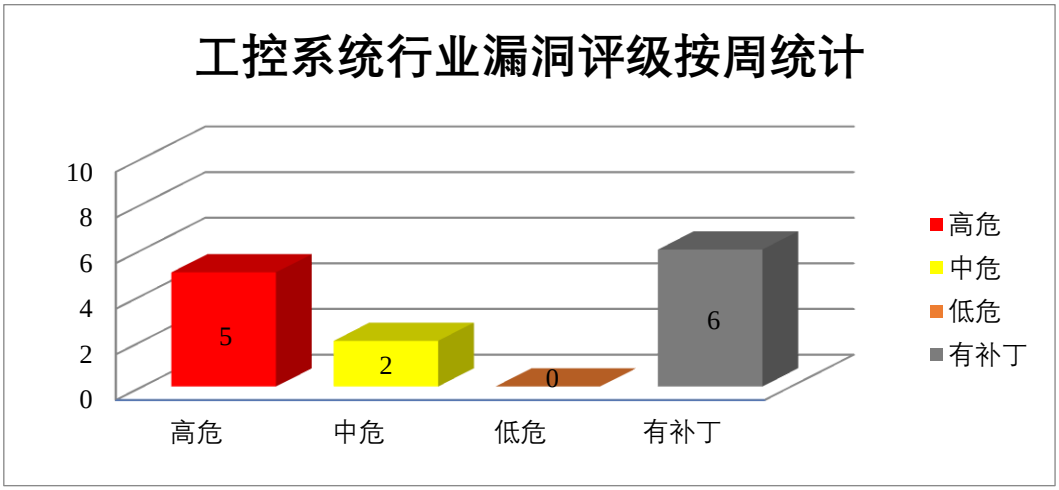

图 5 工控系统行业漏洞统计

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 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，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-34600、CNVD-2024-34599、CNVD-2024-34598、CNVD-2024-34603、CNVD-2024-34602、CNVD-2024-34601、CNVD-2024-34606、CNVD-2024-34605）。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-2024-34600

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34599

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34598

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34603

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34602

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34601

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34606

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34605

2、 Dell 产品安全漏洞

Dell Inventory Collector 是美国戴尔（Dell）公司的一款驱动程序。Dell Peripheral Manager 是一个应用软件。提供了有关如何通过蓝牙将其他设备与计算机配对的屏幕说

明。Dell iDRAC Service Module 是一个轻量级的软件模块，设计用于在 Dell PowerEdge 服务器上运行，以增强 iDRAC（Integrated Dell Remote Access Controller）的功能。Dell InsightIQ 是一个性能监控和报告工具。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信息泄露，执行任意代码，拒绝服务等。

CNVD 收录的相关漏洞包括：Dell Inventory Collector 路径遍历漏洞、Dell Peripheral Manager 不受控搜索路径元素漏洞（CNVD-2024-34486、CNVD-2024-34485）、Dell InsightIQ 加密问题漏洞、Dell iDRAC Service Module 越界写入漏洞（CNVD-2024-34490、CNVD-2024-34494）、Dell iDRAC Service Module 越界读取漏洞（CNVD-2024-34489、CNVD-2024-34492）。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-2024-34487
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34486
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34485
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34492
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34491
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34490
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34489
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34494

3、Google 产品安全漏洞

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，攻击者可利用漏洞通过精心制作的 HTML 页面潜在地利用堆损坏，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2024-34498、CNVD-2024-34496）、Google Chrome 安全绕过漏洞（CNVD-2024-34497）、Google Chrome 释放后重用漏洞（CNVD-2024-34500、CNVD-2024-34502、CNVD-2024-34501）、Google Chrome 输入验证错误漏洞（CNVD-2024-34504）、Google Chrome 越界读取漏洞（CNVD-2024-34499）。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-2024-34498
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34497
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34496
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34500
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34499
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34502

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34501

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34504

4、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，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品信息泄露漏洞、多款 Mozilla 产品代码执行漏洞（CNVD-2024-34588、CNVD-2024-34589）、Mozilla Firefox 和 Thunderbird 安全绕过漏洞（CNVD-2024-34593、CNVD-2024-34596、CNVD-2024-34595）、Mozilla Firefox 和 Thunderbird 代码执行漏洞（CNVD-2024-34594、CNVD-2024-34597）。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-2024-34588

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34590

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34589

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34594

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34593

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34596

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34595

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34597

5、Tenda AX2 Pro 代码执行漏洞

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 被披露存在代码执行漏洞。攻击者可利用该漏洞通过 Routing 功能执行任意代码。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-2024-34973

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-2024-34503	Google Chrome 安全绕过漏洞（CNVD-2024-34503）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html

CNVD-2024-34505	Google Chrome 安全绕过漏洞（CNVD-2024-34505）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_31.html
CNVD-2024-34873	Rockwell Automation PowerFlex 527 输入验证错误漏洞（CNVD-2024-34873）	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/support/advisory.SD1664.html
CNVD-2024-34888	AutomationDirect P3-550E 访问控制错误漏洞（CNVD-2024-34888）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.automationdirect.com/support/software-downloads
CNVD-2024-34889	AutomationDirect P3-550E 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.automationdirect.com/support/software-downloads
CNVD-2024-34918	Microsoft Windows Remote Desktop Licensing 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077
CNVD-2024-34592	多款 Mozilla 产品未经授权访问漏洞	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/mfsa2024-29/ https://www.mozilla.org/security/advisories/mfsa2024-30/ https://www.mozilla.org/security/advisories/mfsa2024-31/ https://www.mozilla.org/security/advisories/mfsa2024-32/
CNVD-2024-34979	SolarWinds Access Rights Manager 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm
CNVD-2024-34982	SolarWinds Access Rights Manager 授权问题漏洞（CNVD-2024-34982）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm
CNVD-2024	SolarWinds Access Rights M	高	厂商已发布了漏洞修复程序，请及

-34981	anager 路径遍历漏洞（CNVD-2024-34981）		时关注更新：https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm

小结：本周，Adobe 产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。此外，Dell、Google、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面潜在地利用堆损坏，获取敏感信息，在系统上执行任意代码或造成拒绝服务等。另外，Tenda AX2 Pro 被披露存在代码执行漏洞。攻击者可利用该漏洞通过 Routing 功能执行任意代码。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、福州网钛软件科技有限公司 idcCMS 跨站请求伪造漏洞

验证描述

idcCMS 是福州网钛软件科技有限公司的一个云管理代理系统。

福州网钛软件科技有限公司 idcCMS 存在跨站请求伪造漏洞，攻击者可利用该漏洞发送错误的 HTTP 请求执行跨站点脚本攻击、Web 缓存中毒和其他恶意活动。

验证信息

POC 链接：https://github.com/FirstLIF/cms/blob/main/2.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-34974

信息提供者

恒安嘉新（北京）科技股份公司

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. AWS 多项服务存在漏洞，能让攻击者完全控制账户

网络安全研究人员在 Amazon Web Services（AWS）产品中发现了多个严重漏洞，如果成功利用这些漏洞，可能会导致严重后果。

参考链接：https://www.freebuf.com/news/408363.html

2. 微软披露 Office 最新零日漏洞，可能导致数据泄露

为了最大程度的规避安全风险，用户应在最终版本的补丁发布后立即更新。

参考链接：https://www.freebuf.com/news/408346.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