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 26 日-2024 年 09 月 01 日 **2024 年第 35 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 362 个，其中高危漏洞 200 个、中危漏洞 151 个、低危漏洞 11 个。漏洞平均分值为 6.80。本周收录的漏洞中，涉及 0day 漏洞 213 个（占 59%），其中互联网上出现“Mini-Tmall SQL 注入漏洞、Tenda G3 缓冲区溢出漏洞”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 33921 个，与上周（44226 个）环比减少 23%。

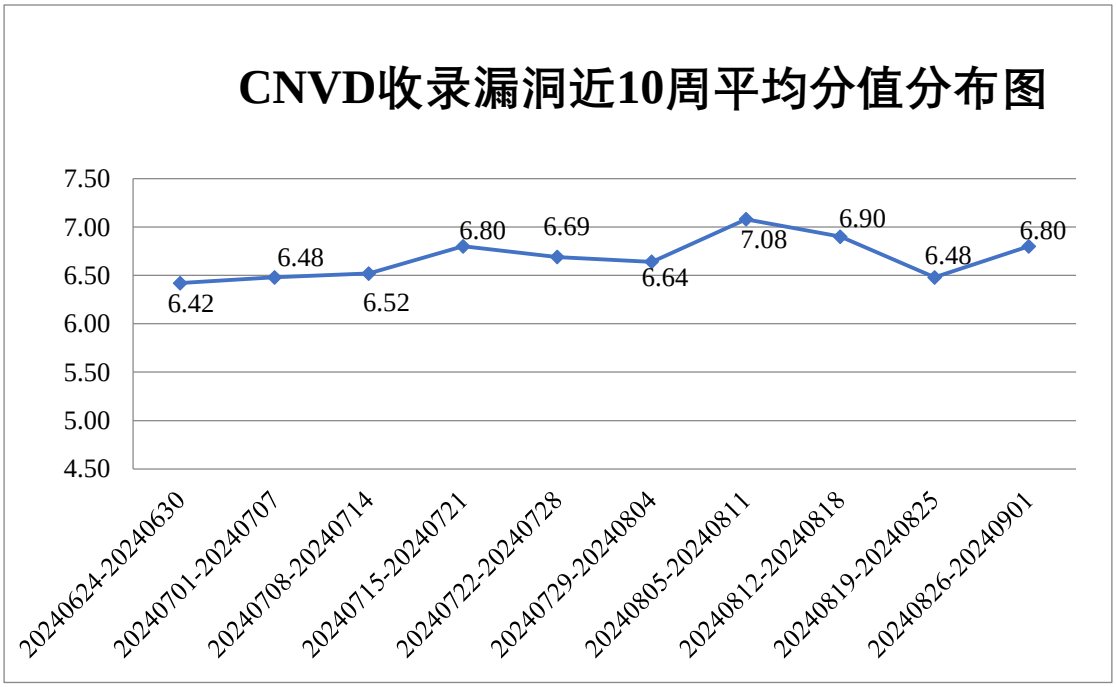

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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，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 660 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 32 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 17 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：

智互联（深圳）科技有限公司、浙江宇视科技有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、武汉噢易云计算股份有限公司、天津天堰科技股份有限公司、天津华远软件科技有限公司、天地（常州）自动化股份有限公司、苏州科达科技股份有限公司、世邦通信股份有限公司、沈阳恩方软件开发有限公司、深圳市同享软件科技有限公司、深圳市普燃计算机软件科技有限公司、深圳市科迈爱康科技有限公司、深圳市吉祥腾达科技有限公司、深圳市鼎游信息技术有限公司、深圳市必联电子有限公司、深圳齐心好视通云计算有限公司、深圳开鸿数字产业发展有限公司、上海普华科技发展股份有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海布雷德科技有限公司、上海百胜软件股份有限公司、善理通益信息科技（深圳）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、厦门甚好软件信息技术有限公司、厦门科拓通讯技术股份有限公司、赛蓝（广州）信息技术有限公司、青岛易软天创网络科技有限公司、奇安信网神信息技术（北京）股份有限公司、联众智慧科技股份有限公司、朗坤智慧科技股份有限公司、昆明奥远科技有限公司、柯尼卡美能达集团、京瓷办公信息系统（中国）有限公司、金润方舟科技股份有限公司、江苏斯普德科技有限公司、济南驰骋信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南创星科技股份有限公司、湖北风拓科技有限公司、杭州盈高科技有限公司、杭州西软信息技术有限公司、杭州品联科技有限公司、哈尔滨新中新电子股份有限公司、贵州小码科技有限公司、广州图创计算机软件开发有限公司、广州华壹智能科技有限公司、广东飞企互联科技股份有限公司、福州银达云创信息科技有限公司、福建引迈信息技术有限公司、畅捷通信息技术股份有限公司、贝尔金贸易（上海）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、北京通达信科科技有限公司、北京时空智友科技有限公司、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、北京谋智火狐信息技术有限公司、北京金和网络股份有限公司、北京和利时集团、北京超图软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、奥琦玮信息科技（北京）有限公司、安美世纪（北京）科技有限公司、安徽新中新华科电子有限公司和安徽科迅教育装备集团有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。杭州海康威视数字技术股份有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、上海观安信息技术股份有限公司、淮安易云科技有限公司、重庆都会信息科技有限公司、成都久信信息技术股份有限公司、北京卓识网安技术股份有限公司、北京神州泰岳软件股份有限公司、河南宝通信息安全测评有限公司、交通运输部南海航海保障中心及其他个人白帽子向 CNVD 提交了 33921 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 32381 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）	20592	20592
奇安信网神（补天平台）	10130	10130
三六零数字安全科技集团有限公司	1181	1181
北京天融信网络安全技术有限公司	1038	0
新华三技术有限公司	807	0
深信服科技股份有限公司	604	6
安天科技集团股份有限公司	546	0
上海交大	478	478
北京神州绿盟科技有限公司	415	0
杭州安恒信息技术股份有限公司	178	145
阿里云计算有限公司	166	0
恒安嘉新（北京）科技股份公司	81	0
北京启明星辰信息安全技术有限公司	67	0
北京知道创宇信息技	22	0

术有限公司		
中国电信集团系统集成有限责任公司	19	19
北京长亭科技有限公司	16	0
杭州迪普科技股份有限公司	10	0
北京安信天行科技有限公司	5	5
远江盛邦（北京）网络安全科技股份有限公司	3	3
南京众智维信息科技有限公司	2	2
北京智游网安科技有限公司	2	2
杭州海康威视数字技术股份有限公司	257	257
河南东方云盾信息技术有限公司	57	57
快页信息技术有限公司	26	26
上海观安信息技术股份有限公司	5	5
淮安易云科技有限公司	3	3
重庆都会信息科技有限公司	2	2
成都久信信息技术股份有限公司	2	2
北京卓识网安技术股份有限公司	1	1
北京神州泰岳软件股份有限公司	1	1
河南宝通信息安全测	1	1

评有限公司		
交通运输部南海航海保障中心	1	1
CNCERT 内蒙古分中心	3	3
CNCERT 宁夏分中心	1	1
个人	998	998
报送总计	37720	33921

本周漏洞按类型和厂商统计

本周，CNVD 收录了 362 个漏洞。WEB 应用 180 个，应用程序 94 个，网络设备（交换机、路由器等网络端设备）55 个，安全产品 14 个，智能设备（物联网终端设备）13 个，数据库 3 个，操作系统 3 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	180
应用程序	94
网络设备（交换机、路由器等网络端设备）	55
安全产品	14
智能设备（物联网终端设备）	13
数据库	3
操作系统	3

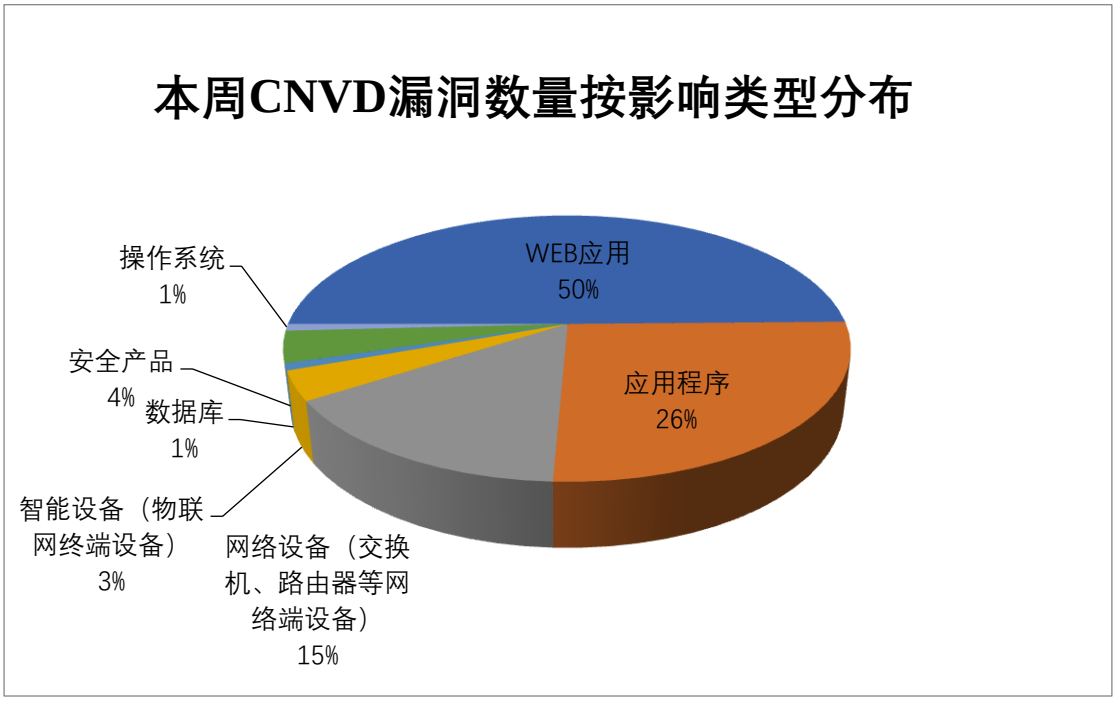

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Mozilla、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	Adobe	22	6%
2	Mozilla	20	6%
3	Microsoft	19	5%
4	用友网络科技股份有限公司	18	5%
5	GTKWave	15	4%
6	畅捷通信息技术股份有限公司	12	3%
7	Tenda	10	3%
8	Broadcom	10	3%
9	Apache	10	3%
10	其他	226	62%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，5 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，“Triangle MicroWorks SCADA Data Gateway 远程代码执行漏洞、Rockwell Automation GuardLogix 5580 和 ControlLogix 5580 拒绝服务漏洞”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/

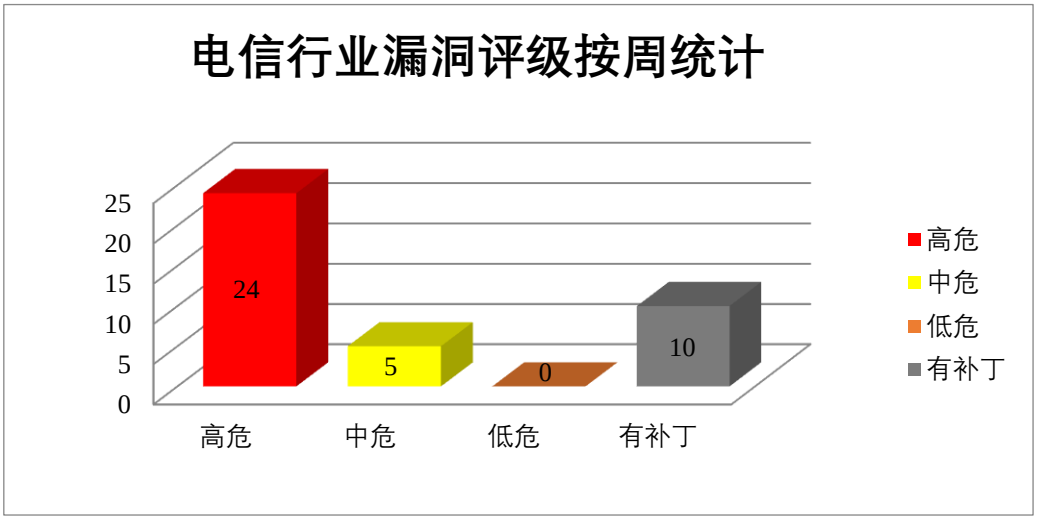

图 3 电信行业漏洞统计

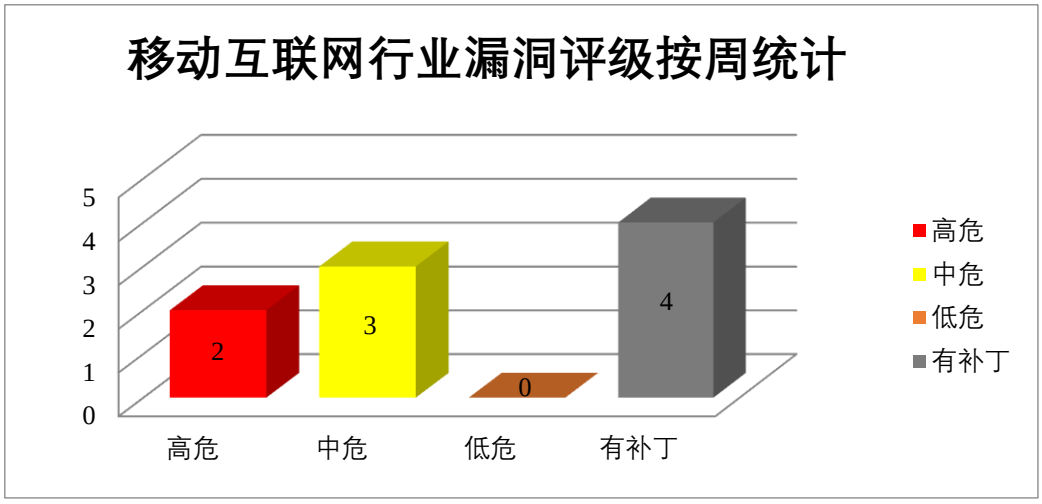

图 4 移动互联网行业漏洞统计

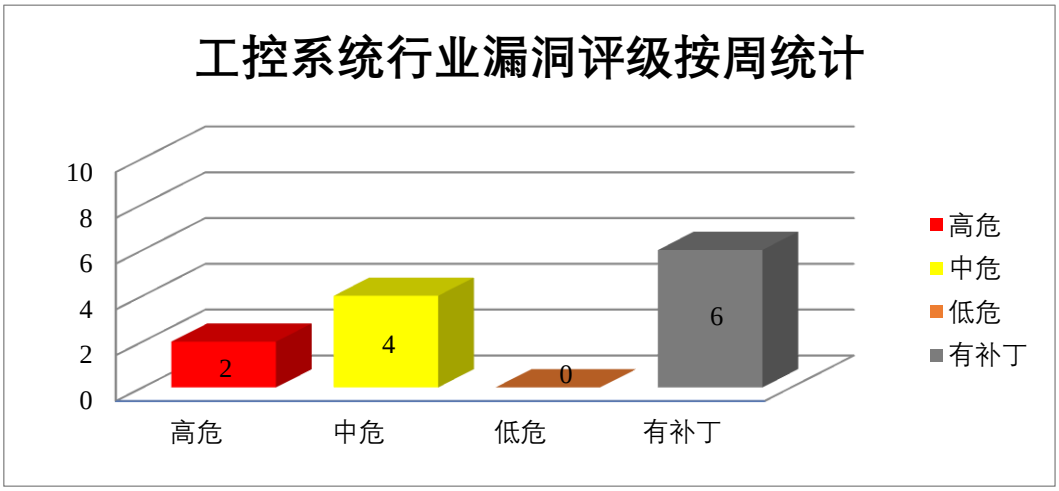

图 5 工控系统行业漏洞统计

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 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 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。Adobe Experience Manager（AEM）是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 Substance 3D Stager 是一个虚拟 3D 工作室。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注入精心设计的有效载荷执行任意 Web 脚本或 HTML，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-36359）、Adobe Commerce 操作系统命令注入漏洞（CNVD-2024-36360）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-36365、CNVD-2024-36364、CNVD-2024-36363、CNVD-2024-36368、CNVD-2024-36367）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2024-36372）。其中，“Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-36359）、Adobe Commerce 操作系统命令注入漏洞（CNVD-2024-36360）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2024-36372）”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-2024-36359
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36360
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36365
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36364
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36363
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36368
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36367
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36372

2、 Apache 产品安全漏洞

Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache DolphinScheduler 是一个分布式的基于 DAG 可视化的工作流任务调度系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行服务器端请求伪造攻击或执行本地脚本，导致服务器进程崩溃等。

CNVD 收录的相关漏洞包括：Apache HTTP Server 输入验证错误漏洞（CNVD-2024-36390）、Apache HTTP Server 代码问题漏洞（CNVD-2024-36389）、Apache HTTP Server 代码执行漏洞、Apache HTTP Server 响应拆分漏洞（CNVD-2024-36394）、Apache HTTP Server 空指针解引用漏洞、Apache HTTP Server 信息泄露漏洞（CNVD-2024-36391）、Apache HTTP Server 输入验证错误漏洞（CNVD-2024-36395）、Apache DolphinScheduler 输入验证错误漏洞（CNVD-2024-36753）。其中，除“Apache HTTP Server 空指针解引用漏洞”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-2024-36390
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36389
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36388
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36394
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36392
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36391
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36395
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36753

3、Microsoft 产品安全漏洞

Microsoft DNS Server 是美国微软（Microsoft）公司的一个服务。Microsoft Windows Remote Desktop Licensing Service 是远程桌面授权服务，允许用户以交互方式连接到远程计算机。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。

CNVD 收录的相关漏洞包括：Microsoft DNS Server 远程代码执行漏洞（CNVD-2024-36374、CNVD-2024-36373、CNVD-2024-36377、CNVD-2024-36376、CNVD-2024-36375、CNVD-2024-36379、CNVD-2024-36378）、Microsoft Windows Remote Desktop Licensing Service 远程代码执行漏洞（CNVD-2024-36381）。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-2024-36374
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36373
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36377
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36376
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36375
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36379
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36378

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36381

4、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。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，在系统上执行任意代码，导致崩溃等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Thunderbird 安全绕过漏洞（CNVD-2024-36722、CNVD-2024-36723）、Mozilla Firefox 和 Thunderbird 代码执行漏洞（CNVD-2024-36724）、Mozilla Firefox 拒绝服务漏洞（CNVD-2024-36727、CNVD-2024-36732）、Mozilla Firefox 代码执行漏洞（CNVD-2024-36730、CNVD-2024-36731）、Mozilla Firefox 代码问题漏洞（CNVD-2024-36765）。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-2024-36722

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36723

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36724

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36727

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36730

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36731

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36732

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36765

5、TOTOLINK LR350 命令注入漏洞

TOTOLINK LR350 是中国吉翁电子（TOTOLINK）公司的一款无线路由器。本周，TOTOLINK LR350 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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-2024-36757

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-2024-36380	Microsoft Windows Remote Desktop Licensing Service 拒绝服务漏洞（CNVD-2024-36380）	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-2024-38072
CNVD-2024-36386	Microsoft Windows Remote Desktop Licensing Service 拒	高	厂商已发布了漏洞修复程序，请及时关注更新：

	绝服务漏洞		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073
CNVD-2024-36715	Mozilla Firefox for iOS 安全绕过漏洞（CNVD-2024-36715）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2024-36/
CNVD-2024-36719	Mozilla Firefox 和 Thunderbird 信息泄露漏洞	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/
CNVD-2024-36720	Mozilla Firefox for Android 权限提升漏洞	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/
CNVD-2024-36737	Tenda FH1206 formSafeEmailFilter 函数栈溢出漏洞	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://www.tenda.com.cn/product/overview/FH1206.html
CNVD-2024-36741	Microsoft Azure Health Bot 存在权限提升漏洞	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38109
CNVD-2024-36752	Foxit PDF Reader 内存错误引用远程代码执行漏洞	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.foxit.com/support/security-bulletins.html
CNVD-2024-36760	Fortinet FortiADC 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.fortinet.com/psirt/FG-IR-22-298
CNVD-2024-36909	Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2024-36909）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.adobe.com/acrobat/pdf-reader.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞发通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，执行任意代码等。此外，Apache、Microsoft、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提获取敏感信息，执行服务器端请求伪造攻击或执行本地脚本，在系统上执行任意代码，导致服务器进程崩溃等。另外，TOTOLINK LR350 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命

令执行。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 G3 缓冲区溢出漏洞

验证描述

Tenda G3 是中国腾达（Tenda）公司的一款 Qos Vpn 路由器。

Tenda G3 存在缓冲区溢出漏洞，经过身份验证的远程，攻击者可利用该漏洞溢出缓冲区并在系统上执行任意代码，或者导致应用程序崩溃。

验证信息

POC 链接：https://github.com/abcdefg-png/IoT-vulnerable/blob/main/Tenda/G3/G3V15/modifyDhcpRule.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-36945

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. Fortra 针对 FileCatalyst Workflow 安全漏洞发布补丁

Fortra 解决了影响 FileCatalyst Workflow 的安全漏洞，远程攻击者可能会滥用该漏洞来获得管理访问权限。该漏洞被跟踪为 CVE-2024-6633，CVSS 评分为 9.8，源于使用静态密码连接到 HSQL 数据库。

参考链接：https://thehackernews.com/2024/08/fortra-issues-patch-for-high-risk.html

2. 开源 GPS 系统曝出两个安全漏洞

披露的两个漏洞都是路径遍历（PathTraversal）漏洞，当启用访客注册功能（Traccar5 的默认配置）时，漏洞就会被武器化利用。

参考链接：https://www.secrss.com/articles/69519

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