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 09 日-2024 年 09 月 15 日 **2024 年第 37 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 261 个，其中高危漏洞 142 个、中危漏洞 112 个、低危漏洞 7 个。漏洞平均分值为 6.78。本周收录的漏洞中，涉及 0day 漏洞 171 个（占 66%），其中互联网上出现“Tenda F1202 fromwebExcptypemanFilter 函数堆栈缓冲区溢出漏洞、TOTOLINK X5000R 和 A7000R 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 28055 个，与上周（7902 个）环比增加 255%。

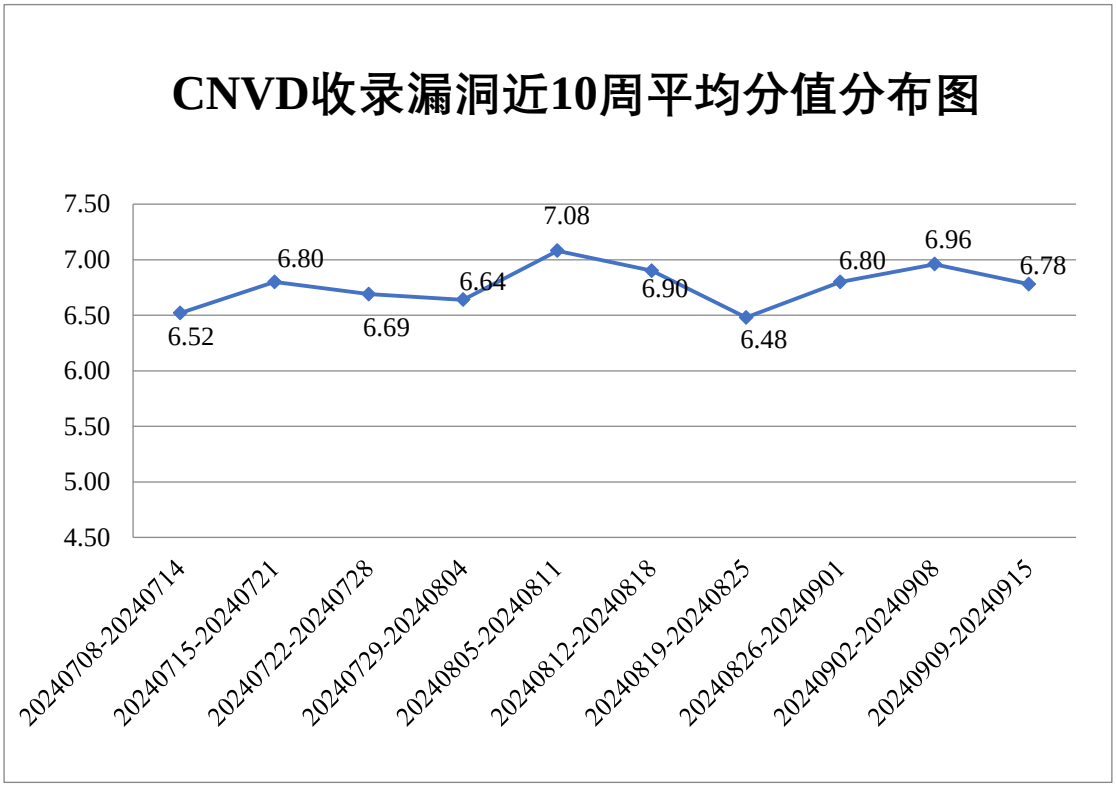

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 3 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 493 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 57 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：

浙江和达科技股份有限公司、漳州市芗城帝兴软件开发有限公司、云南达远软件有限公司、云和恩墨（北京）信息技术有限公司、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、信呼、新天科技股份有限公司、新道科技股份有限公司、小米科技有限责任公司、西安众邦网络科技有限公司、武汉华信数据系统有限公司、通州区华丽软件工作室、天地（常州）自动化股份有限公司、太原福莱瑞达物流设备科技有限公司、索尼（中国）有限公司、松下电器（中国）有限公司、施耐德电气（中国）有限公司、深圳拓安信物联股份有限公司、深圳市中兴新云服务有限公司、深圳市优特普科技有限公司、深圳市伊林思科技有限公司、深圳市赛格导航科技股份有限公司、深圳市磊科实业有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、上海知备信息科技有限公司、上海三高计算机中心股份有限公司、上海穆云智能科技有限公司、上海顶想信息科技有限公司、上海贝锐信息科技股份有限公司、上海百胜软件股份有限公司、山东比特智能科技股份有限公司、厦门宇电自动化科技有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、青岛三利集团有限公司、青岛东胜伟业软件有限公司、麒麟软件有限公司、普联技术有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、理光（中国）投资有限公司、乐普（北京）医疗器械股份有限公司、乐金电子（中国）有限公司、乐创未来（武汉）科技有限公司、柯尼卡美能达集团、江阴汇智软件技术有限公司、江西铭软科技有限公司、江苏称意智能科技有限公司、吉翁电子（深圳）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、泓华国际医疗控股有限公司、杭州三一谦成科技有限公司、杭州品联科技有限公司、杭州荷花软件有限公司、杭州短链网络技术有限公司、汉王科技股份有限公司、贵州小码科技有限公司、广州小橘灯信息科技有限公司、广州市保伦电子有限公司、广州和晖科技有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、泛微网络科技股份有限公司、东芝（中国）有限公司、畅捷通信息技术股份有限公司、北京字节跳动科技有限公司、北京中识科技有限公司、北京中广上洋科技股份有限公司、北京中犇科技有限公司、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、北京小米科技有限责任公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京金和网络股份有限公司、北京国炬信息技术有限公司、北京飞易腾科技有限公司、北京

碧虚文化有限公司、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、爱普生（中国）有限公司、SeaCMS 和 Lexmark。

本周，CNVD 发布了《Microsoft 发布 2024 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/10411

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、新华三技术有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、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。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、淮安易云科技有限公司、北京翰慧投资咨询有限公司、信息产业信息安全测评中心、苏州棱镜七彩信息科技有限公司、中资网络信息安全科技有限公司、快页信息技术有限公司、江苏正信信息安全测试有限公司、北京天下信安技术有限公司、马鞍山书拓安全科技有限公司、北京山石网科信息技术有限公司、广州华南检验检测中心有限公司、江苏极元信息技术有限公司、成都久信信息技术股份有限公司、联想集团、厦门聚丁科技有限公司、成都安美勤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、北京卓识网安技术股份有限公司、江苏软测信息科技有限公司、泸州职业技术学院、福建浩程信息科技有限公司、陕西慧缘网络科技有限公司、联通数字科技有限公司、江苏晟晖信息科技有限公司、深圳市佰航信息技术有限公司及其他个人白帽子向 CNVD 提交了 28055 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 26409 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）	23493	23493
三六零数字安全科技集团有限公司	2507	2507
北京启明星辰信息安全技术有限公司	1603	0
新华三技术有限公司	1083	0
深信服科技股份有限公司	641	0
北京天融信网络安全技术有限公司	483	8

北京神州绿盟科技有限公司	483	1
上海交大	409	409
安天科技集团股份有限公司	317	0
中国电信股份有限公司网络安全产品运营中心	238	238
北京数字观星科技有限公司	197	0
京东科技信息技术有限公司	164	1
阿里云计算有限公司	164	0
远江盛邦（北京）网络安全科技股份有限公司	104	104
恒安嘉新（北京）科技股份公司	82	0
杭州迪普科技股份有限公司	29	0
杭州安恒信息技术股份有限公司	27	1
北京知道创宇信息技术有限公司	27	0
中国电信集团系统集成有限责任公司	7	3
华为技术有限公司	5	5
北京长亭科技有限公司	1	1
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	218	218
西门子（中国）有限公司	22	0

河南东方云盾信息技术有限公司	31	31
淮安易云科技有限公司	13	13
北京翰慧投资咨询有限公司	13	13
信息产业信息安全测评中心	13	13
苏州棱镜七彩信息科技有限公司	6	6
中资网络信息安全科技有限公司	6	6
快页信息技术有限公司	4	4
江苏正信信息安全测试有限公司	5	5
北京天下信安技术有限公司	4	4
马鞍山书拓安全科技有限公司	4	4
北京山石网科信息技术有限公司	4	4
广州华南检验检测中心有限公司	3	3
江苏极元信息技术有限公司	3	3
成都久信信息技术股份有限公司	3	3
联想集团	2	2
厦门聚丁科技有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2

北京卓识网安技术股份有限公司	1	1
江苏软测信息科技有限公司	1	1
泸州职业技术学院	1	1
福建浩程信息科技有限公司	1	1
陕西慧缘网络科技有限公司	1	1
联通数字科技有限公司	1	1
江苏晟晖信息科技有限公司	1	1
深圳市佰航信息技术有限公司	1	1
个人	937	937
报送总计	33370	28055

本周漏洞按类型和厂商统计

本周，CNVD 收录了 261 个漏洞。WEB 应用 154 个，应用程序 50 个，网络设备（交换机、路由器等网络端设备）37 个，操作系统 14 个，数据库 3 个，智能设备（物联网终端设备）2 个，安全产品 1 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	154
应用程序	50
网络设备（交换机、路由器等网络端设备）	37
操作系统	14
数据库	3
智能设备（物联网终端设备）	2
安全产品	1

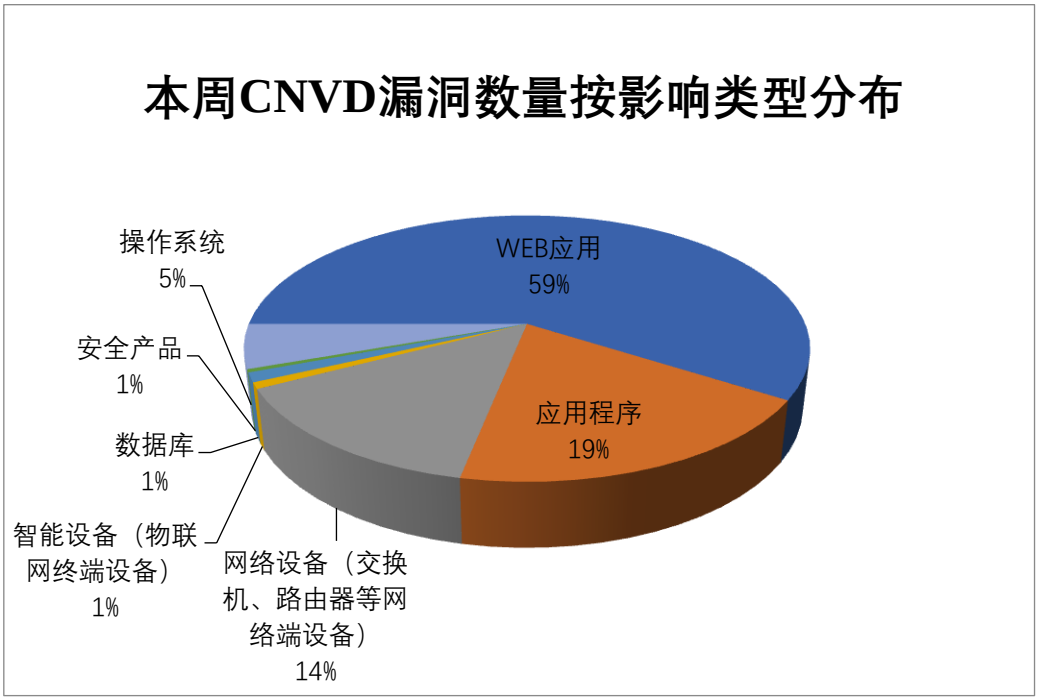

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SIEMENS、GTKWave、用友网络科技股份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	SIEMENS	22	8%
2	GTKWave	17	6%
3	用友网络科技股份有限公司	15	6%
4	Warehouse Inventory System	13	5%
5	Google	12	5%
6	Cisco	10	4%
7	Adobe	8	3%
8	畅捷通信息技术股份有限公司	7	3%
9	智互联（深圳）科技有限公司	6	2%
10	其他	151	58%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，11 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2024-37972）、

Tenda AC10U fromSetRouteStatic 函数缓冲区溢出漏洞”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/

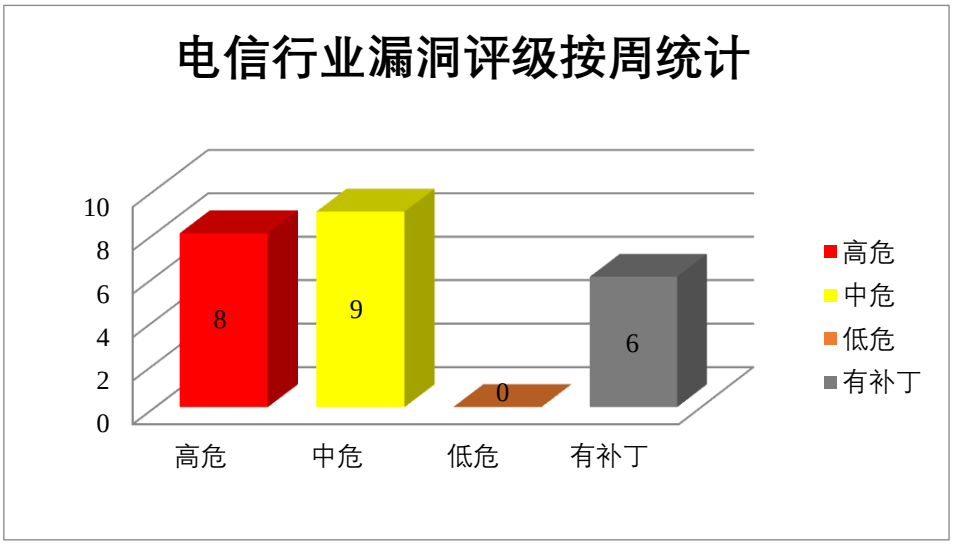

图 3 电信行业漏洞统计

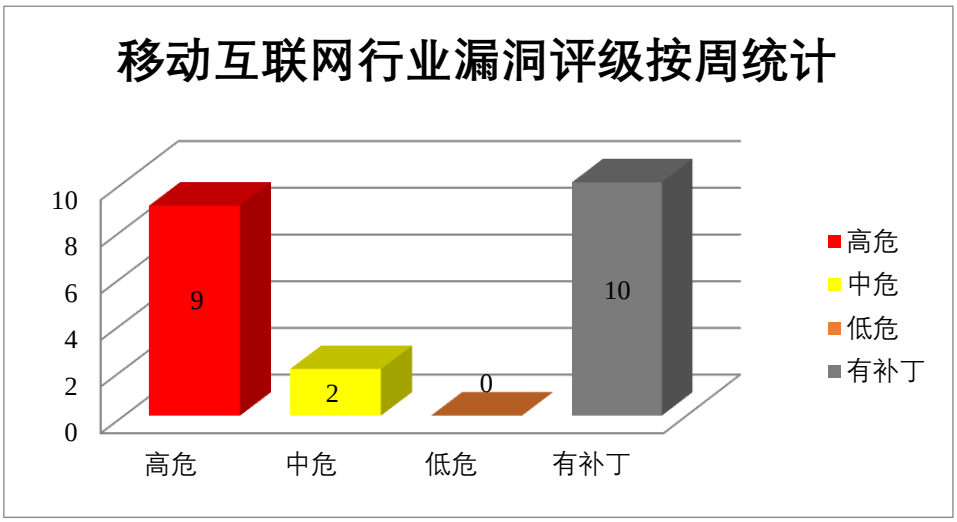

图 4 移动互联网行业漏洞统计

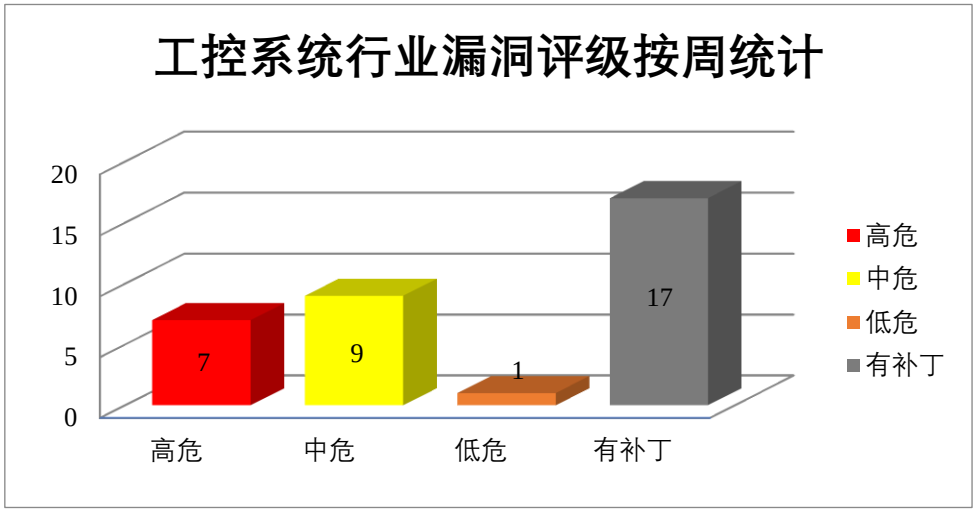

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Google Chrome 越界写入漏洞（CNVD-2024-37813）、Google Chrome 内存错误引用漏洞（CNVD-2024-37814）、Google Android 权限提升漏洞（CNVD-2024-37966、CNVD-2024-37968、CNVD-2024-37970、CNVD-2024-37969、CNVD-2024-37971）、Google Android 拒绝服务漏洞（CNVD-2024-37967）。其中，除“Google Android 权限提升漏洞（CNVD-2024-37966）”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-2024-37813

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37814

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37966

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37968

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37967

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37970

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37969

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37971

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。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功能，通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，导致内存泄露。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 输入验证错误漏洞（CNVD-2024-37805）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37808、CNVD-2024-37807、CNVD-2024-37806、CNVD-2024-37811、CNVD-2024-37810、CNVD-2024-37809）、Adobe Acrobat and Reader 越界读取漏洞（CNVD-2024-37812）。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-2024-37805

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37808

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37807

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37806

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37811

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37810

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37809

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37812

3、 Cisco 产品安全漏洞

Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco Identity Services Engine 是美国思科(Cisco)公司的一款环境感知平台。Cisco Unified Communications Manager 是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。Cisco Nexus Dashboard 是美国思科（Cisco）公司的一个单一控制台。能够简化数据中心网络的运营和管理。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪造恶意请求诱骗受害者点击执行敏感操作，提升权限，执行任意命令，导致系统拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco NX-OS Software 命令执行漏洞、Cisco NX-OS Software 拒绝服务漏洞（CNVD-2024-37698）、Cisco Identity Services Engine 跨站请求伪造漏洞（CNVD-2024-37703、CNVD-2024-37706）、Cisco Unified Communications Manager 跨站脚本漏洞（CNVD-2024-37702）、Cisco NX-OS Software 授权问题漏洞（CNVD-2024-37701）、Cisco NX-OS Software 权限提升漏洞（CNVD-2024-37700）、

Cisco Nexus Dashboard 跨站请求伪造漏洞。其中，“Cisco NX-OS Software 拒绝服务漏洞（CNVD-2024-37698）、Cisco Identity Services Engine 跨站请求伪造漏洞（CNVD-2024-37703、CNVD-2024-37706）、Cisco Nexus Dashboard 跨站请求伪造漏洞”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-2024-37699
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37698
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37703
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37702
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37701
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37700
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37707
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37706

4、Siemens 产品安全漏洞

Siemens SINEMA Remote Connect Server 是德国西门子（Siemens）公司的一套远程网络管理平台。该平台主要用于远程访问、维护、控制和诊断底层网络。S7-200 SMART series 是一系列微型可编程逻辑控制器，可以控制各种小型自动化应用。Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。SINUMERIK CNC 为车间、车间和大型批量生产环境提供自动化解决方案。SINUMERIK ONE 是一个数字原生数控系统，集成了 SIMATIC S7-1500 CPU，用于自动化。Siemens Industrial Edge Management 是德国西门子（Siemens）公司的一个平台，用于在靠近车间的计算平台上托管来自不同供应商的应用程序。Siemens Automation License Manager 是德国西门子（Siemens）公司的一款用于 Siemens 产品的许可证管理器。SIMATIC PCS neo 是一个分布式控制系统（DCS）。SINEC NMS 是面向数字企业的新一代网络管理系统（NMS）。该系统可用于集中监控、管理和配置网络。Totally Integrated Automation Portal (TIA Portal)是一款 PC 软件，提供对西门子全方位数字化自动化服务的访问，从数字规划和集成工程到透明操作。User Management Component (UMC)是一个集成组件，可以在系统范围内对用户进行集中维护。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用户会话建立的额外多因素身份验证，获取敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens SINEMA Remote Connect Server 会话固定漏洞、Siemens SIMATIC S7-200 SMART Devices 拒绝服务漏洞、Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞（CNVD-2024-38014）、Siemens SINUMERIK ONE、SINUMERIK-840D 和 SINUMERIK828D 权限提升漏洞、Siemens Industrial Edge

Management 授权绕过漏洞、Siemens SINUMERIK 系统日志信息泄露漏洞、Siemens Automation License Manager 拒绝服务漏洞、Siemens User Management Component (UMC) 堆缓冲区溢出漏洞。其中，除“Siemens SINEMA Remote Connect Server 会话固定漏洞、Siemens SINUMERIK 系统日志信息泄露漏洞”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-2024-38005
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38004
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38006
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38014
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38021
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38020
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38023
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38022
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38025

5、Tenda AX1806 缓冲区溢出漏洞（CNVD-2024-38182）

Tenda AX1806 是中国腾达（Tenda）公司的一个 WiFi6 无线路由器。本周，Tenda AX1806 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞导致拒绝服务。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-2024-38182

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-2024-37731	GTKWave 整数溢出漏洞（CNVD-2024-37731）	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-2024-37752	GTKWave 整数溢出漏洞（CNVD-2024-37752）	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-2024-37967	Google Android 拒绝服务漏洞（CNVD-2024-37967）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2024-08-01
CNVD-2024	Google Android 权限提升漏	高	厂商已发布了漏洞修复程序，请及

-37972	洞（CNVD-2024-37972）		时关注更新：https://source.android.com/security/bulletin/2024-08-01
CNVD-2024-37974	Google Android Framework 权限提升漏洞（CNVD-2024-37974）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2024-06-01
CNVD-2024-38013	Siemens SIMATIC SCADA 和 PCS 7 systems 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-629254.html
CNVD-2024-38022	Siemens Automation License Manager 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-103653.html
CNVD-2024-38188	GTKWave 整数溢出漏洞（CNVD-2024-38188）	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-2024-38197	NetIQ Advanced Authentication 暴力破解漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netiq.com/documentation/advanced-authentication-63/advanced-authentication-releasenotes-6351/data/advanced-authentication-releasenotes-6351.html
CNVD-2024-38201	NetIQ Advanced Authentication 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netiq.com/documentation/advanced-authentication-63/advanced-authentication-releasenotes-6351/data/advanced-authentication-releasenotes-6351.html

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上执行任意代码，导致拒绝服务。此外，Adobe、Cisco、Siemens 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功能，获取敏感信息，提升权限，执行任意命令，导致拒绝服务等。另外，Tenda AX1806 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞导致拒绝服务。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 F1202 fromwebExcptypemanFilter 函数堆栈缓冲区溢出漏洞

验证描述

Tenda F1202 是一款网络设备，提供网络连接和数据传输功能。

Tenda F1202 fromwebExcptypemanFilter 函数存在堆栈缓冲区溢出漏洞，该漏洞是由于/goform/webExctypemanFilter 文件的 webExctypeman Filter 函数的边界检查不正确造成的。攻击者可利用该漏洞使缓冲区溢出，并在系统上执行任意代码。

验证信息

POC 链接：https://github.com/abcdefg-png/IoT-vulnerable/blob/main/Tenda/F/F1202/fromwebExcptypemanFilter.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-38184

信息提供者

华为技术有限公司

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. 苹果 Vision Pro 曝出安全漏洞，黑客可通过用户眼动输入窃取信息

近日，苹果公司的 Vision Pro 混合现实头戴式设备曝出一个安全漏洞，一旦被黑客成功利用，他们就可以推断出用户在该设备的虚拟键盘上输入的具体数据。

参考链接：https://www.freebuf.com/news/411003.html

2. WhatsApp“阅后即焚”功能曝安全漏洞，黑客可反复查看

据 BleepingComputer 消息，全球拥有 20 亿用户的即时通讯工具 WhatsApp 最近修复了一个十分重要的隐私漏洞，该漏洞能允许攻击者多次查看用户发送的“阅后即焚”（View once）内容。

参考链接：https://www.freebuf.com/news/410675.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