

## 信息安全漏洞周报

2024年03月18日-2024年03月24日

2024年第12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 497 个，其中高危漏洞 221 个、中危漏洞 264 个、低危漏洞 12 个。漏洞平均分为 6.56。本周收录的漏洞中，涉及 0day 漏洞 405 个（占 81%），其中互联网上出现“Tenda AC 10U formSetPPTPServer 函数缓冲区溢出漏洞、Delinea PAM Secret Server 信息泄露漏洞”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 5953 个，与上周（12519 个）环比减少 52%。

### CNVD收录漏洞近10周平均分分布图

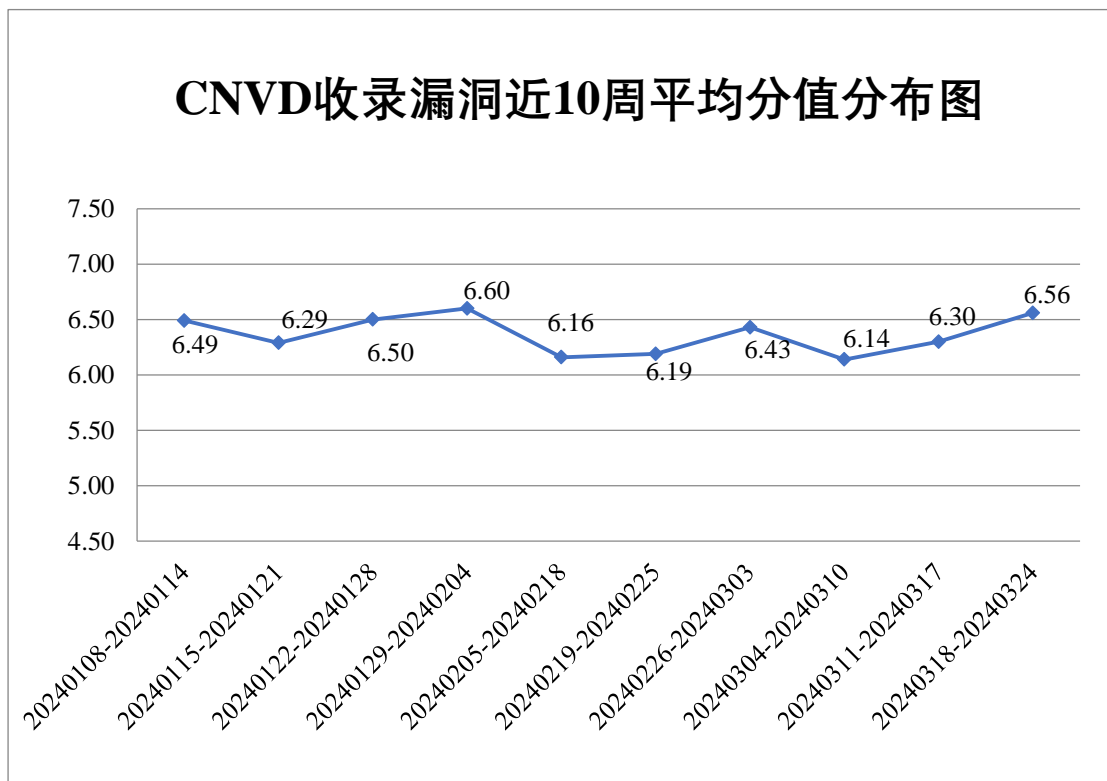


图 1 CNVD 收录漏洞近 10 周平均分分布图


### 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 10 起，向基础电信企业通报漏洞事件 13 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 256 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 63 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 21 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：

佐藤自动识别系统国际贸易（上海）有限公司、紫光软件系统有限公司、珠海市同海科技股份有限公司、重庆远秋科技股份有限公司、中科数字通（北京）科技有限公司、智慧芽信息科技（苏州）有限公司、智互联（深圳）科技有限公司、智邦大陆科技有限公司、正方软件股份有限公司、浙江中控技术股份有限公司、浙江零跑科技股份有限公司、浙江工企信息技术股份有限公司、长城汽车股份有限公司、漳州市芴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、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、新晨科技股份有限公司、夏普商贸（中国）有限公司、西安众邦网络科技有限公司、西安瑞友信息技术资讯有限公司、西安大西信息科技有限公司、武汉天地伟业科技有限公司、武汉达梦数据库有限公司、威海市天罡仪表股份有限公司、万洲电气股份有限公司、苏州科达科技股份有限公司、苏州汉明科技有限公司、松下电器（中国）有限公司、沈阳点动科技有限公司、深圳智慧光迅信息技术有限公司、深圳维盟网络技术有限公司、深圳拓安信物联股份有限公司、深圳市拓普泰尔科技有限公司、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、深圳市科脉技术股份有限公司、深圳市科迈爱康科技有限公司、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、深圳市顶讯网络科技有限公司、深圳市道尔智控科技股份有限公司、深圳锐取信息技术股份有限公司、深圳力维智联技术有限公司、深圳警翼智能科技股份有限公司、深圳鼎信通达股份有限公司、上海易教科技股份有限公司、上海迅饶自动化科技有限公司、上海尚强信息科技有限公司、上海开始网络科技有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、山东运筹软件有限公司、山东潍微科技股份有限公司、山东迪彩商贸有限公司、山东比特智能科技股份有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、麒麟软件有限公司、奇安信网神信息技术（北京）股份有限公司、邳州天目网络科技有限公司、绵阳探云科技有限公司、龙采科技集团有限责任公司、蓝卓数字科技有限公司、蓝网科技股份有限公司、江苏省捷达科技发展有限公司、江苏赛达电子科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖北楚天智能交通股份有限公司、河南润土信息科技有限公司、河北先河环保科技股份有限公司、杭州瑞利声电技术有限公司、

杭州可道云网络有限公司、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、广州易达建信科技开发有限公司、广州图创计算机软件开发有限公司、广州璐华信息技术有限公司、广州宏天软件股份有限公司、广州红帆科技有限公司、广西方略网络技术有限公司、广东保伦电子股份有限公司、福建科立讯通信有限公司、帆软软件有限公司、东华软件股份公司、东莞市通天星软件科技有限公司、成都星锐蓝海网络科技有限公司、成都极企科技有限公司、成都德芯数字科技股份有限公司、畅捷通信息技术股份有限公司、贝尔金国际有限公司、北京中软国际教育科技股份有限公司、北京中科聚网信息技术有限公司、北京中成科信科技发展有限公司、北京中犇科技有限公司、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、北京微步在线科技有限公司、北京网瑞达科技有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京世纪超星信息技术发展有限责任公司、北京神州数码云科信息技术有限公司、北京派网软件有限公司、北京龙软科技股份有限公司、北京猎鹰安全科技有限公司、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、北京华宇信息技术有限公司、北京宏景世纪软件股份有限公司、北京汉王智远科技有限公司、北京冠新医卫软件科技有限公司、北京东方华盾信息技术有限公司、北京北大方正电子有限公司、北京邦永科技有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽省科迅教育装备有限公司、Delta Electronics, Inc.和爱普生（中国）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、北京数字观星科技有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。河南东方云盾信息技术有限公司、贵州多彩网安科技有限公司、中孚安全技术有限公司、联通数字科技有限公司、甘肃赛飞安全科技有限公司、快页信息技术有限公司、江苏金盾检测技术股份有限公司、北京山石网科信息技术有限公司、吉林省吉林祥云信息技术有限公司、江苏极元信息技术有限公司、内蒙古中叶信息技术有限责任公司、西藏熙安信息技术有限责任公司、江苏云天网络安全技术有限公司、北京微步在线科技有限公司、河南灵创电子科技有限公司、江苏晟晖信息科技有限公司、星云博创科技有限公司、中国软件评测中心、联想集团、中电福富信息科技有限公司、中资网络信息安全科技有限公司、统信软件技术有限公司、安徽天行网安信息安全技术有限公司、湖南泛联新安信息科技有限公司、北银金融科技有限责任公司、成都愚安科技有限公司、瑞数信息技术（上海）有限公司、海南神州希望网络有限公司、中国电信股份有限公司上海研究院、北京时代新威信息技术有限公司、

贵州华黔信安信息技术有限公司、广西塔易信息技术有限公司、天津市兴先道科技有限公司、上海直画科技有限公司、信联科技（南京）有限公司、杭州孝道科技有限公司、陕西慧缘网络科技有限公司、深圳昂楷科技有限公司、博智安全科技股份有限公司、北京天防安全科技有限公司、中电万维信息技术有限责任公司、广州中科诺泰技术有限公司、深圳市魔方安全科技有限公司、江苏天创科技有限公司、江西中和证信息安全技术有限公司、建信金融科技有限责任公司（建信金科网络攻击实验室）、山东云天安全技术有限公司、国网上海市电力公司及其他个人白帽子向 CNVD 提交了 5953 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）和上海交大向 CNVD 共享的白帽子报送的 4270 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
北京天融信网络安全技术有限公司	2628	1
斗象科技(漏洞盒子)	2468	2468
奇安信网神（补天平台）	1299	1299
新华三技术有限公司	1005	0
深信服科技股份有限公司	705	0
上海交大	503	503
北京数字观星科技有限公司	393	0
安天科技集团股份有限公司	299	4
阿里云计算有限公司	275	5
北京神州绿盟科技有限公司	213	1
北京启明星辰信息安全技术有限公司	174	14
北京知道创宇信息技术有限公司	160	0
中国电信集团系统集成有限责任公司	82	3
北京安信天行科技有限公司	65	65

杭州安恒信息技术股份有限公司	42	1
恒安嘉新（北京）科技股份有限公司	30	0
北京长亭科技有限公司	26	5
杭州迪普科技股份有限公司	10	0
远江盛邦（北京）网络安全科技股份有限公司	4	4
北京智游网安科技有限公司	3	3
北京升鑫网络科技有限公司（青藤云）	1	1
浙江大华技术股份有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
河南东方云盾信息技术有限公司	40	40
中电科网络安全科技股份有限公司	40	0
贵州多彩网安科技有限公司	37	37
中孚安全技术有限公司	29	29
联通数字科技有限公司	18	18
甘肃赛飞安全科技有限公司	13	13
快页信息技术有限公司	11	11
江苏金盾检测技术股份有限公司	11	11

北京山石网科信息技术有限公司	9	9
吉林省吉林祥云信息技术有限公司	8	8
江苏极元信息技术有限公司	6	6
内蒙古中叶信息技术有限责任公司	6	6
西藏熙安信息技术有限公司	5	5
江苏云天网络安全技术有限公司	4	4
北京微步在线科技有限公司	4	4
河南灵创电子科技有限公司	4	4
江苏晟晖信息科技有限公司	4	4
星云博创科技有限公司	4	4
中国软件评测中心	4	4
联想集团	3	3
中电福富信息科技有限公司	3	3
中资网络信息安全科技有限公司	3	3
统信软件技术有限公司	3	3
安徽天行网安信息安全技术有限公司	3	3
湖南泛联新安信息科技有限公司	3	3
北银金融科技有限责任公司	3	3
成都愚安科技有限公司	2	2

司		
瑞数信息技术(上海)有限公司	2	2
海南神州希望网络有限公司	2	2
中国电信股份有限公司上海研究院	2	2
北京时代新威信息技术有限公司	2	2
贵州华黔信安信息技术有限公司	2	2
广西塔易信息技术有限公司	2	2
天津市兴先道科技有限公司	1	1
上海直画科技有限公司	1	1
信联科技(南京)有限公司	1	1
杭州孝道科技有限公司	1	1
陕西慧缘网络科技有限公司	1	1
深圳昂楷科技有限公司	1	1
博智安全科技股份有限公司	1	1
北京天防安全科技有限公司	1	1
中电万维信息技术有限责任公司	1	1
广州中科诺泰技术有限公司	1	1
深圳市魔方安全科技有限公司	1	1

江苏天创科技有限公司	1	1
江西中和证信息安全技术有限公司	1	1
建信金融科技有限责任公司（建信金科网络攻击实验室）	1	1
山东云天安全技术有限公司	1	1
国网上海市电力公司	1	1
CNCERT 浙江分中心	24	24
CNCERT 河北分中心	6	6
个人	1276	1276
报送总计	12001	5953

### 本周漏洞按类型和厂商统计

本周，CNVD 收录了 497 个漏洞。WEB 应用 262 个，应用程序 115 个，网络设备（交换机、路由器等网络端设备）78 个，智能设备（物联网终端设备）21 个，操作系统 15 个，安全产品 4 个，数据库 2 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	262
应用程序	115
网络设备（交换机、路由器等网络端设备）	78
智能设备（物联网终端设备）	21
操作系统	15
安全产品	4
数据库	2



## 本周CNVD漏洞数量按影响类型分布

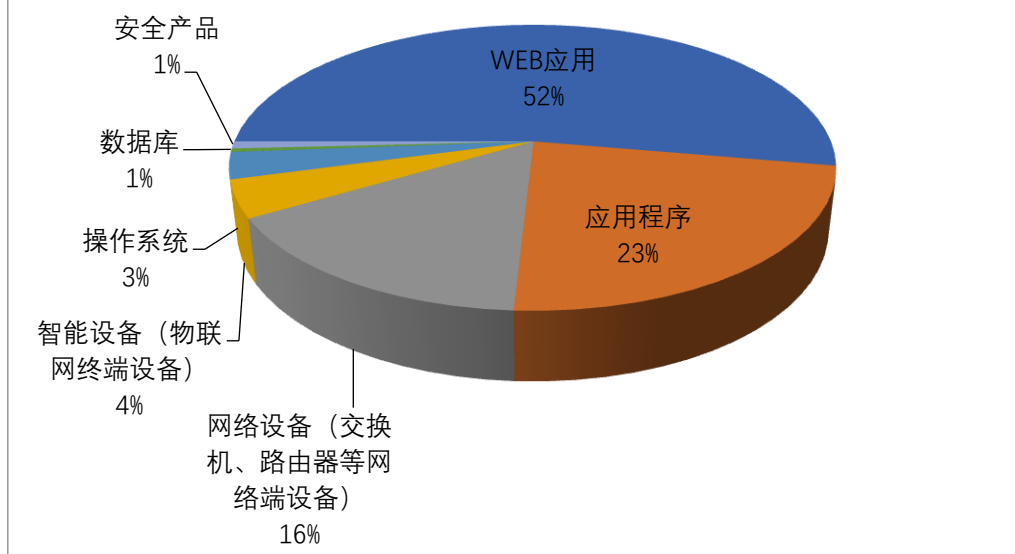


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京百卓网络技术有限公司、用友网络科技股份有限公司、Tenda 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	北京百卓网络技术有限公司	21	4%
2	用友网络科技股份有限公司	20	4%
3	Tenda	19	4%
4	北京亿赛通科技发展有限公司	16	3%
5	Google	14	3%
6	北京星网锐捷网络技术有限公司	12	2%
7	Customer Support System	11	2%
8	Apache	10	2%
9	Fortinet	10	2%
10	其他	364	74%

## 本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，47 个移动互联网行业漏洞，12 个工控行

业漏洞（如下图所示）。其中，“Tenda AC18 fromSetWirelessRepeat 函数缓冲区溢出漏洞、Google Android Framework 权限提升漏洞（CNVD-2024-13745）、Siemens SINEMA Remote Connect Server 访问控制错误漏洞（CNVD-2024-13805）”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/>

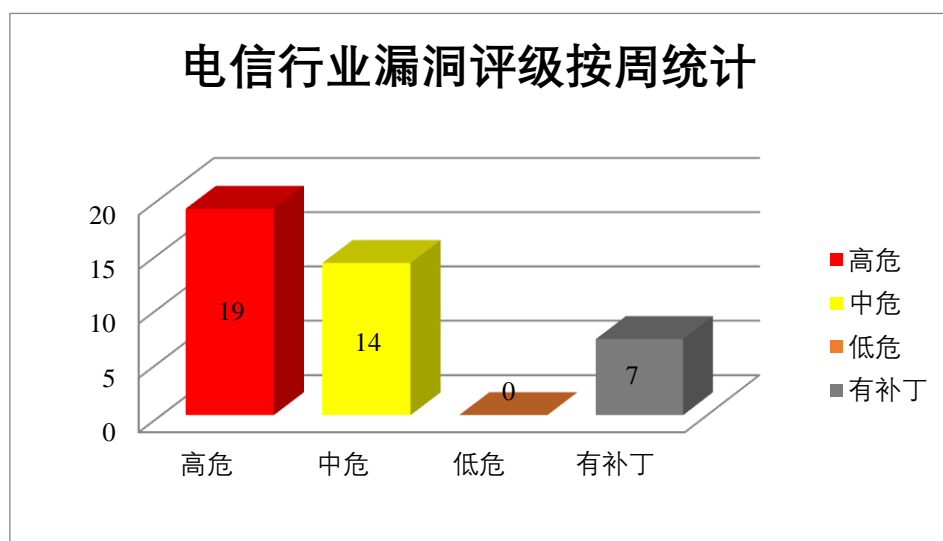


图3 电信行业漏洞统计

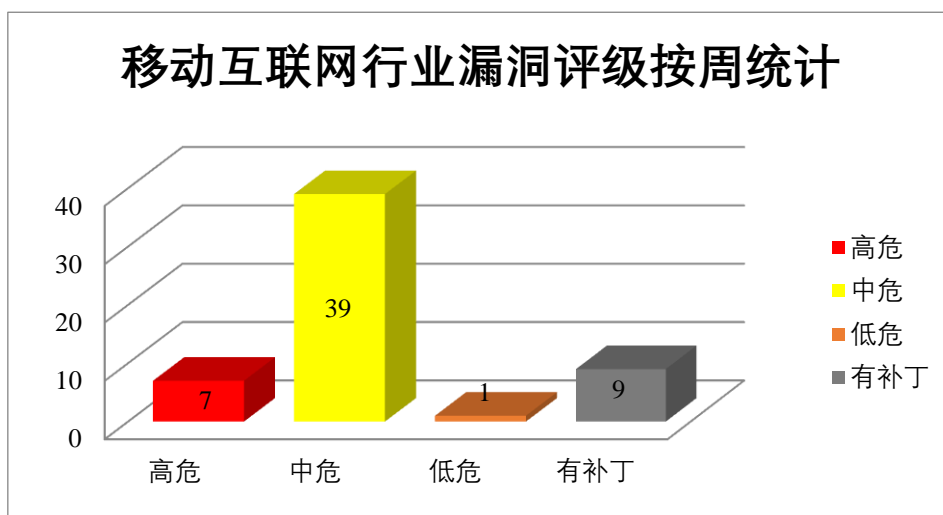


图4 移动互联网行业漏洞统计

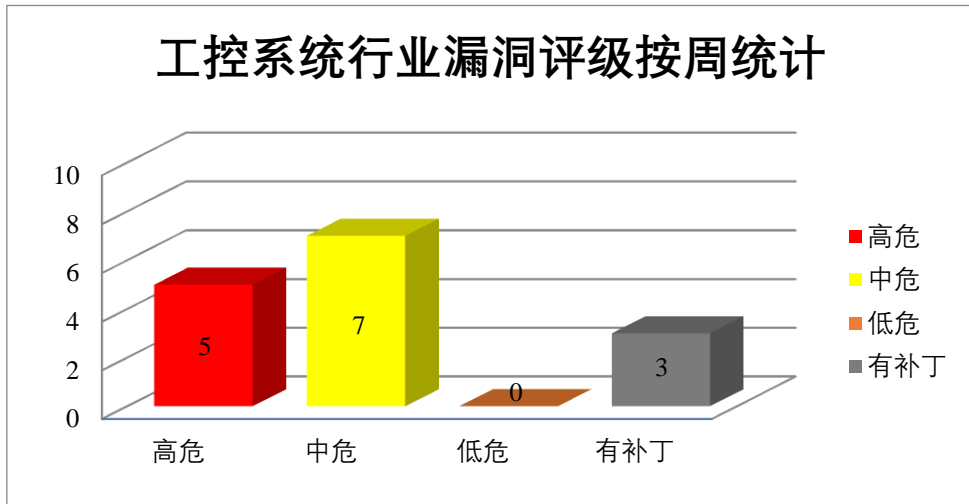


图 5 工控系统行业漏洞统计

## 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 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，攻击者可利用漏洞获取敏感信息，升级权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2024-13714、CNVD-2024-13716）、Google Android 信息泄露漏洞（CNVD-2024-13744）、Google Android Framework 权限提升漏洞（CNVD-2024-13745、CNVD-2024-13746）、Google Chrome 代码执行漏洞（CNVD-2024-13759）、Google Chrome 越界写入漏洞（CNVD-2024-13760）、Google Chrome 代码执行漏洞（CNVD-2024-13761）。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-2024-13714>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13716>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13744>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13745>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13746>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13759>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13760>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13761>

### 2、Fortinet 产品安全漏洞

Fortinet FortiManager 是美国飞塔 (Fortinet) 公司的一套集中化网络安全管理平台。该平台支持集中管理任意数量的 Fortinet 设备, 并能够将设备分组到不同的管理域 (ADOM) 进一步简化多设备安全部署与管理。Fortinet FortiClientEMS 是美国飞塔 (Fortinet) 公司的 Fortinet 提供的端点管理解决方案的一部分, 旨在帮助组织有效地管理其网络中的终端设备, 并提供端点安全性的监控和控制。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。Fortinet FortiClient 是美国飞塔 (Fortinet) 公司的一套移动终端安全解决方案。该方案与 FortiGate 防火墙设备连接时可提供 IPsec 和 SSL 加密、广域网优化、终端合规和双因子认证等功能。Fortinet FortiSIEM 是美国飞塔 (Fortinet) 公司的一套安全信息和事件管理系统。该系统包括资产发现、工作流程自动化和统一管理等功能。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞执行非法 SQL 命令窃取数据库敏感数据, 通过特制的 HTTP 请求可以执行未经授权的代码或命令, 导致拒绝服务等。

CNVD 收录的相关漏洞包括: Fortinet FortiManager 访问控制错误漏洞 (CNVD-2024-13750)、Fortinet FortiClientEMS SQL 注入漏洞、Fortinet FortiOS 缓冲区溢出漏洞 (CNVD-2024-13748)、Fortinet FortiOS and FortiProxy 输入验证错误漏洞 (CNVD-2024-13755)、Fortinet FortiOS and FortiProxy 拒绝服务漏洞、Fortinet FortiClient 授权问题漏洞、Fortinet FortiOS and FortiProxy 缓冲区溢出漏洞、Fortinet FortiSIEM 命令执行漏洞 (CNVD-2024-13756)。其中, 除“Fortinet FortiOS and FortiProxy 输入验证错误漏洞 (CNVD-2024-13755)、Fortinet FortiOS and FortiProxy 拒绝服务漏洞、Fortinet FortiClient 授权问题漏洞”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-2024-13750>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13749>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13748>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13755>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13754>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13753>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13751>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13756>

### 3、Apache 产品安全漏洞

Apache Tomcat 是美国阿帕奇 (Apache) 基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page (JSP) 的支持。Apache Airflow 是美国阿帕奇 (Apache) 基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩

展和动态监控等特点。Apache Airflow 是美国阿帕奇 (Apache) 基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。Apache Doris 是美国阿帕奇 (Apache) 基金会的现代 MPP 分析数据库产品。Apache Answer 是美国阿帕奇 (Apache) 基金会的社区平台。Apache Dolphinscheduler 是美国阿帕奇 (Apache) 基金会的现代数据编排平台。Apache DolphinScheduler 是美国阿帕奇 (Apache) 基金会的分布式的基于 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，攻击者可利用漏洞绕过访问限制，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Tomcat 输入验证错误漏洞、Apache Airflow 信息泄露漏洞 (CNVD-2024-13567)、Apache Airflow 信任管理问题漏洞 (CNVD-2024-13571)、Apache Doris 信息泄露漏洞 (CNVD-2024-13570)、Apache Tomcat 拒绝服务漏洞 (CNVD-2024-13569)、Apache Answer 拒绝服务漏洞、Apache DolphinScheduler 安全绕过漏洞、Apache Dolphinscheduler 任意文件读取漏洞。其中，除“Apache Airflow 信息泄露漏洞 (CNVD-2024-13567)、Apache Answer 拒绝服务漏洞”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-2024-13568>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13567>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13571>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13570>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13569>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13573>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13577>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13576>

#### 4、Siemens 产品安全漏洞

Siemens Siveillance Control 是德国西门子 (Siemens) 公司的一款集成了视频监控、门禁、入侵检测等功能的安全管理平台，旨在帮助组织实现对建筑物、设施和人员的全面监控和管理。Cerberus PRO EN 是一个由防火板、探测和管理站组成的消防系统。它可供西门子合作伙伴使用，并符合欧洲标准 EN 54 中关于火灾探测和报警系统的规定。

Sinteso EN 是一个由防火板、检测和管理站组成的消防系统。它符合火灾探测和报警系统的欧洲标准 EN 54。Sinteso Mobile 是用于远程访问 Sinteso/Cerberus PRO EN 消防系统的移动应用程序。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。SINEMA Remote Connect 是一个用于远程网络的管理平台，能够简单管理总部、服务技术人员和已安装机器或工厂之间的隧道连接 (VPN)。SENTRON PAC Me

ter 产品是用于精确能源管理和透明信息采集的功率测量设备。Siemens Simcenter Femap 是德国西门子（Siemens）公司的一款尖端工程学仿真应用程序。用于创建、编辑和导入/重用复杂产品或系统基于网格的有限元分析模型。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，以 root 权限在底层操作系统上执行代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens Siveillance Control 授权绕过漏洞、Siemens Sinteso EN 和 Cerberus PRO EN Fire Protection Systems 堆栈缓冲区溢出漏洞、Siemens Sinteso EN 和 Cerberus PRO EN Fire Protection Systems 越界读取漏洞、Siemens Sinteso EN 和 Cerberus PRO EN Fire Protection Systems 缓冲区溢出漏洞、Siemens SINEMA Remote Connect Server 访问控制错误漏洞（CNVD-2024-13805）、Siemens SINEMA Remote Connect Client 信息泄露漏洞、Siemens SENTRON 7KM PAC3x20 Devices 访问控制不当漏洞、Siemens Simcenter Femap 缓冲区溢出漏洞（CNVD-2024-13809）。其中，除“Siemens Siveillance Control 授权绕过漏洞、Siemens SINEMA Remote Connect Client 信息泄露漏洞、Siemens SENTRON 7KM PAC3x20 Devices 访问控制不当漏洞”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-2024-13801>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13802>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13803>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13804>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13805>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13806>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13807>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13809>

## 5、TOTOLINK EX1800T 命令执行漏洞

TOTOLINK EX1800T 是中国吉翁电子（TOTOLINK）公司的一款 Wi-Fi 范围扩展器。本周，TOTOLINK EX1800T 被披露存在命令执行漏洞，攻击者可利用该漏洞在系统上执行任意命令。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-2024-13794>

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	Discourse 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时

-14090			时关注更新： <a href="https://github.com/discourse/discourse/security/advisories/GHSA-hf2v-r5xm-8p37">https://github.com/discourse/discourse/security/advisories/GHSA-hf2v-r5xm-8p37</a>
CNVD-2024-14307	Mattermost 授权问题漏洞（CNVD-2024-14307）	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://mattermost.com/security-updates/">https://mattermost.com/security-updates/</a>
CNVD-2024-14309	Tenda AC18 fromSetWireless Repeat 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://github.com/rnmods/react-native-document-picker">https://github.com/rnmods/react-native-document-picker</a>
CNVD-2024-14313	Tenda W9 越界写入漏洞（CNVD-2024-14313）	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.tenda.com.cn/">https://www.tenda.com.cn/</a>
CNVD-2024-14371	Tenda W9 越界写入漏洞（CNVD-2024-14371）	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.tenda.com.cn/download/detail-2986.html">https://www.tenda.com.cn/download/detail-2986.html</a>
CNVD-2024-14374	Tenda AC9 缓冲区溢出漏洞（CNVD-2024-14374）	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.tenda.com.cn/download/detail-2908.html">https://www.tenda.com.cn/download/detail-2908.html</a>
CNVD-2024-14579	GeoServer 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://github.com/geoserver/geoserver/security/advisories/GHSA-9v5q-2gwq-q9hq">https://github.com/geoserver/geoserver/security/advisories/GHSA-9v5q-2gwq-q9hq</a>
CNVD-2024-14582	LibHTTP 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： <a href="https://github.com/OISF/libhttp/security/advisories/GHSA-f9wf-rrjj-qx8m">https://github.com/OISF/libhttp/security/advisories/GHSA-f9wf-rrjj-qx8m</a>
CNVD-2024-14587	Tenda i6 formSetCfm 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.tendacn.com/download/detail-2771.html">https://www.tendacn.com/download/detail-2771.html</a>
CNVD-2024-14589	GeoServer 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： <a href="https://docs.geoserver.org/stable/en/user/services/wps/operations.html#execute">https://docs.geoserver.org/stable/en/user/services/wps/operations.html#execute</a>

小结：本周，Google 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，升级权限，在系统上执行任意代码。此外，Fortinet、Apache、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访问限制，获取敏感信息，以 root 权限在底层操作系统上执行代码，导致拒绝服务等。另外，TOTOLINK EX1800T 被披露存在命令执行漏洞，攻击者可利用该漏洞在系统上执行任意命令。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 AC10U formSetPPTPServer 函数缓冲区溢出漏洞

#### 验证描述

Tenda AC10U 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10U formSetPPTPServer 函数存在缓冲区溢出漏洞，该漏洞源于 formSetPPTPServer 函数的 startIp 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://github.com/yaoyue123/iot/blob/main/Tenda/AC10U/formSetPPTPSe  
rver.md](https://github.com/yaoyue123/iot/blob/main/Tenda/AC10U/formSetPPTPSe<br/>rver.md)

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2024-13798>

#### 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. AWS 曝一键式漏洞，攻击者可接管 Apache Airflow 服务

近日，AWS 修复了一个关键漏洞，通过利用该漏洞，攻击者可直接接管亚马逊 Apache Airflow（MWAA）托管工作流。该漏洞危害较大，虽然利用起来比较复杂，但仍建议及时进行修复。

参考链接：<https://www.freebuf.com/news/395687.html>

### 2. UDP 协议被曝漏洞：可被利用发起拒绝服务攻击

CISPA Helmholtz 信息安全中心的安全专家近日发布报告，称在用户数据报协议（UDP）中发现安全漏洞，追踪编号为 CVE-2024-2169，利用该漏洞的攻击者会创建一个自我持续机制，无限制地产生过大流量，且无法阻止，从而导致目标系统甚至整个网络出



现拒绝服务（DoS）情况。

参考链接：<https://www.ithome.com/0/757/132.htm>

### 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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82991537