# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2022 年 11 月 07 日-2022 年 11 月 13 日** **2022 年第 45 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 405 个，其中高危漏洞 172 个、中危漏洞 169 个、低危漏洞 64 个。漏洞平均分值为 6.09。本周收录的漏洞中，涉及 0day 漏洞 311 个（占 77%），其中互联网上出现“FacturaScripts 跨站脚本漏洞（CNVD-2022-76230）、Survey Sparrow Enterprise Survey Software 跨站脚本漏洞”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事件型漏洞总数 18262 个，与上周（16853 个）环比增加 8%。

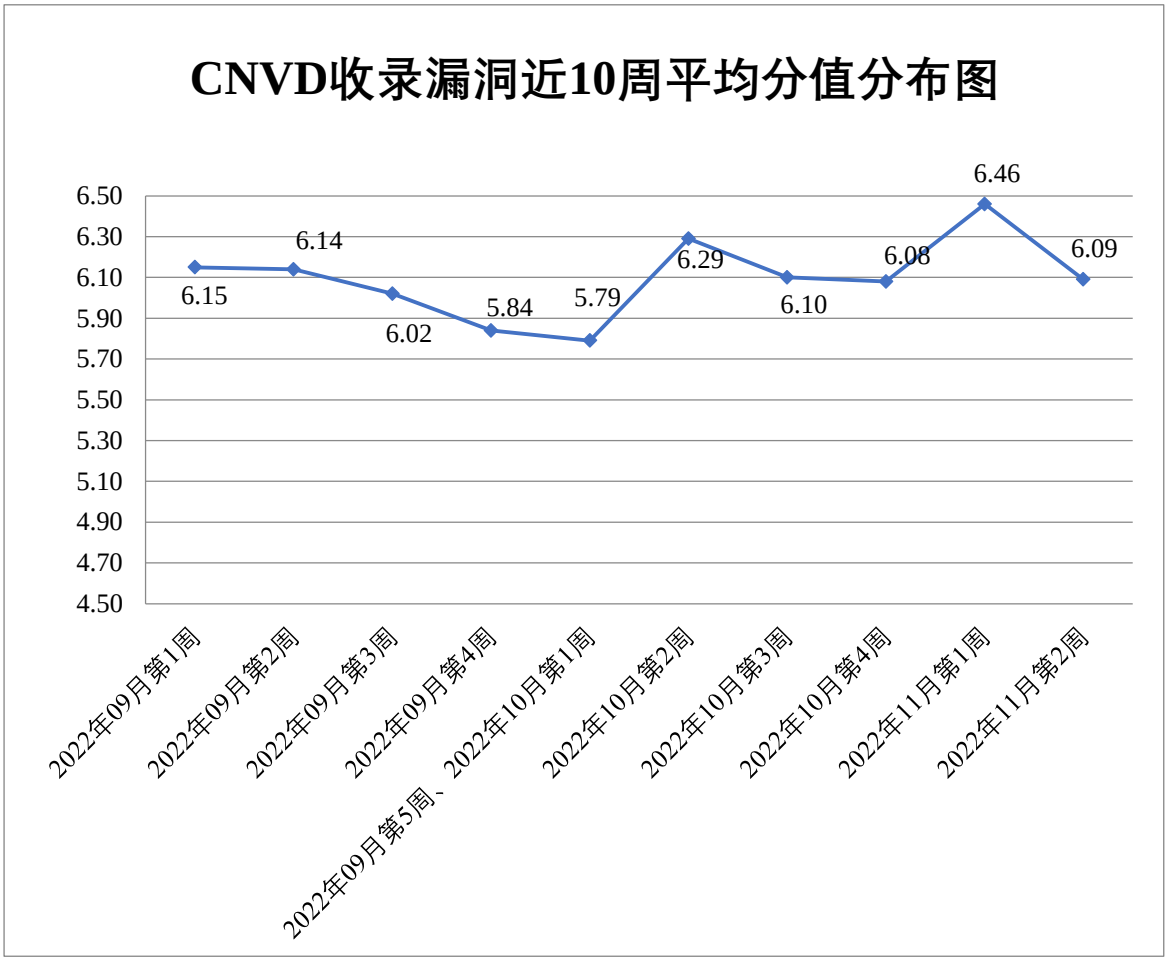

图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 42 起，向基础电信企业通报漏洞事件 53 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 743 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 175 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 154 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：

紫光云技术有限公司、珠海玖时光科技有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆梅安森科技股份有限公司、重庆泛普软件有限公司、正星氢电科技郑州有限公司、浙江宇视科技有限公司、浙江用安软件有限公司、浙江乐檬信息技术有限公司、浙江大华技术股份有限公司、浙江标点信息科技有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、徐州亿优网架钢结构工程有限公司、熊猫智慧水务有限公司、兄弟（中国）商业有限公司、新秀科技、新疆云景网络科技有限公司、武汉秒开网络科技有限公司、武汉达梦数据库有限公司、望海康信（北京）科技股份公司、天津神州浩天科技有限公司、苏州遇见信息科技有限公司、苏州天一信德环保科技有限公司、苏州汉明科技有限公司、四川迅睿云软件开发有限公司、曙光信息产业股份有限公司、深圳智沃科技有限公司、深圳维盟科技股份有限公司、深圳市欣博跃电子有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市东宝信息技术有限公司、深圳昂楷科技有限公司、上海卓卓网络科技有限公司、上海宜同贸易有限公司、上海锐昉科技有限公司、上海荃路软件开发工作室、上海灵当信息科技有限公司、上海共情网络科技有限公司、上海斐讯数据通信技术有限公司、山西峰凡科技物流有限公司、山东欧倍尔软件科技有限责任公司、山东康程信息科技有限公司、厦门网中网软件有限公司、青岛易企天创管理咨询有限公司、青岛海信网络科技股份有限公司、启明星辰信息技术集团股份有限公司、鹏展万国电子商务（深圳）有限公司、宁波智仪通能源科技有限公司、南京涌亿思信息技术有限公司、良心网文化传播有限公司、联奕科技股份有限公司、浪潮通用软件有限公司、廊坊市极致网络科技有限公司、竣禾科技、京源中科科技股份有限公司、金蝶软件（中国）有限公司、江西金磊科技发展有限公司、江苏省广电有线信息网络股份有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、湖南强智科技发展有限公司、湖南创星科技股份有限公司、湖南翱云网络科技有限公司、红厨帽国际广告传媒（北京）有限公司、弘扬软件股份有限公司、河南中设智控信息科技有限公司、河南开云信息技

术有限公司、杭州易软共创网络科技有限公司、杭州图特信息科技有限公司、杭州三汇信息工程有限公司、杭州吉拉科技有限公司、杭州冠航科技有限公司、杭州短趣网络传媒技术有限公司、哈尔滨伟成科技有限公司、贵州筑站信息技术有限公司、贵州万峰林智慧旅游有限公司、广州网易计算机系统有限公司、广州图创计算机软件发展有限公司、广州斯必得电子科技有限公司、广州南方卫星导航仪器有限公司、广州恒企教育科技有限公司、广东全程云科技有限公司、福州联讯信息科技有限公司、东莞市一码网络科技有限公司、大连华天软件有限公司、北京致远互联软件股份有限公司、北京亿心宜行汽车技术开发服务有限公司、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、北京万户网络技术有限公司、北京天融信网络安全技术有限公司、北京数字政通科技股份有限公司、北京世纪超星信息技术发展有限责任公司、北京青牛技术股份有限公司、北京诺码信科技有限公司、北京久幺幺科技有限公司、北京建恒信安科技有限公司、北京华宇信息技术有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、安徽共生物流科技有限公司、阿里巴巴集团安全应急响应中心、TOTOLINK、seacms、Netis Systems、Lexmark、BEESCMS 和 Amazon Web Services, Inc.。

本周，CNVD 发布了《Microsoft 发布 2022 年 11 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8276

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司、深信服科技股份有限公司、南京众智维信息科技有限公司等单位报送公开收集的漏洞数量较多。北京升鑫网络科技有限公司、中国电信股份有限公司网络安全产品运营中心、北京云科安信科技有限公司（Seraph 安全实验室）、河南东方云盾信息技术有限公司、北京山石网科信息技术有限公司、北京安盟信息技术股份有限公司、安徽锋刃信息科技有限公司、杭州迪普科技股份有限公司、杭州默安科技有限公司、河南信安世纪科技有限公司、河南灵创电子科技有限公司、苏州棱镜七彩信息科技有限公司、山石网科通信技术股份有限公司、北京华顺信安信息技术有限公司、山东云天安全技术有限公司、江苏保旺达软件技术有限公司、浙江木链物联网科技有限公司、北京微步在线科技有限公司、重庆都会信息科技、山东新潮信息技术有限公司、贵州多彩网安科技有限公司、上海纽盾科技股份有限公司、博智安全科技股份有限公司、山东九域信息技术有限公司、苏州众里数码科技有限公司、湖北珞格科技发展有限公司、西安敏恒信息技术有限公司、杭州美创科技有限公司、内蒙古信元网络安全技术股份有限公司、云南联创网安科技有限公司、山东正中信息技术股份有限公司、中通服创发科

技有限责任公司、西安秦易信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司及其他个人白帽子向 CNVD 提交了 18262 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）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 16579 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 |
|---|---|---|
| 斗象科技（漏洞盒子） | 8729 | 8729 |
| 奇安信网神（补天平台） | 5585 | 5585 |
| 三六零数字安全科技集团有限公司 | 1533 | 1533 |
| 上海交大 | 732 | 732 |
| 新华三技术有限公司 | 463 | 4 |
| 北京神州绿盟科技有限公司 | 313 | 0 |
| 安天科技集团股份有限公司 | 282 | 0 |
| 深信服科技股份有限公司 | 215 | 0 |
| 南京众智维信息科技有限公司 | 147 | 147 |
| 北京启明星辰信息安全技术有限公司 | 146 | 1 |
| 西安四叶草信息技术有限公司 | 144 | 144 |
| 天津市国瑞数码安全系统股份有限公司 | 118 | 0 |
| 恒安嘉新（北京）科技股份公司 | 101 | 0 |
| 北京数字观星科技有限公司 | 101 | 0 |
| 西门子（中国）有限公司 | 30 | 0 |
| 中国电信集团系统集成有限责任公司 | 27 | 0 |

| | | |
|---|---|---|
| 远江盛邦（北京）网络安全科技股份有限公司 | 11 | 11 |
| 卫士通信息产业股份有限公司 | 11 | 11 |
| 内蒙古云科数据服务股份有限公司 | 6 | 6 |
| 北京长亭科技有限公司 | 5 | 5 |
| 京东科技信息技术有限公司 | 5 | 5 |
| 北京天融信网络安全技术有限公司 | 3 | 3 |
| 深圳市腾讯计算机系统有限公司（玄武实验室） | 2 | 2 |
| 北京知道创宇信息技术有限公司 | 1 | 1 |
| 北京升鑫网络科技有限公司 | 74 | 74 |
| 中国电信股份有限公司网络安全产品运营中心 | 65 | 65 |
| 北京云科安信科技有限公司（Seraph 安全实验室） | 61 | 61 |
| 河南东方云盾信息技术有限公司 | 58 | 58 |
| 北京山石网科信息技术有限公司 | 31 | 31 |
| 北京安盟信息技术股份有限公司 | 30 | 30 |
| 安徽锋刃信息科技有限公司 | 26 | 26 |
| 杭州迪普科技股份有 | 26 | 5 |

| | | |
|---|---|---|
| 限公司 | | |
| 杭州默安科技有限公司 | 23 | 23 |
| 河南信安世纪科技有限公司 | 15 | 15 |
| 河南灵创电子科技有限公司 | 11 | 11 |
| 苏州棱镜七彩信息科技有限公司 | 11 | 11 |
| 山石网科通信技术股份有限公司 | 6 | 6 |
| 北京华顺信安信息技术有限公司 | 6 | 6 |
| 山东云天安全技术有限公司 | 5 | 5 |
| 江苏保旺达软件技术有限公司 | 5 | 5 |
| 浙江木链物联网科技有限公司 | 5 | 5 |
| 北京微步在线科技有限公司 | 5 | 5 |
| 重庆都会信息科技 | 4 | 4 |
| 山东新潮信息技术有限公司 | 4 | 4 |
| 贵州多彩网安科技有限公司 | 4 | 4 |
| 上海纽盾科技股份有限公司 | 4 | 4 |
| 博智安全科技股份有限公司 | 2 | 2 |
| 山东九域信息技术有限公司 | 2 | 2 |
| 苏州众里数码科技有限公司 | 2 | 2 |
| 湖北珞格科技发展有 | 2 | 2 |

| | | |
|---|---|---|
| 限公司 | | |
| 西安敏恒信息技术有限公司 | 1 | 1 |
| 杭州美创科技有限公司 | 1 | 1 |
| 内蒙古信元网络安全技术股份有限公司 | 1 | 1 |
| 云南联创网安科技有限公司 | 1 | 1 |
| 山东正中信息技术股份有限公司 | 1 | 1 |
| 中通服创发科技有限责任公司 | 1 | 1 |
| 西安秦易信息技术有限公司 | 1 | 1 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 1 | 1 |
| 个人 | 868 | 868 |
| 报送总计 | 20074 | 18262 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 405 个漏洞。WEB 应用 170 个，应用程序 115 个，网络设备（交换机、路由器等网络端设备）83 个，智能设备（物联网终端设备）19 个，操作系统 11 个，安全产品 7 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 | 170 |
| 应用程序 | 115 |
| 网络设备（交换机、路由器等网络端设备） | 83 |
| 智能设备（物联网终端设备） | 19 |
| 操作系统 | 11 |
| 安全产品 | 7 |

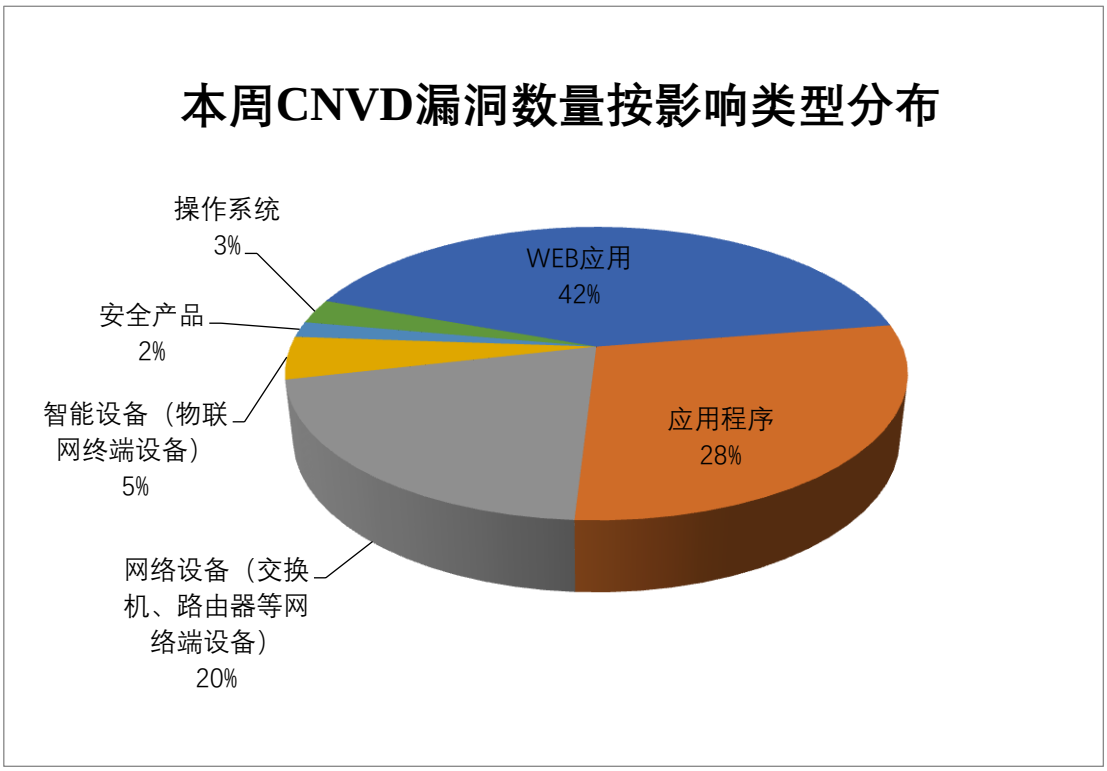


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 TOTOLINK、Siemens、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 | TOTOLINK | 17 | 4% |
| 2 | Siemens | 15 | 4% |
| 3 | Tenda | 15 | 4% |
| 4 | Samsung | 15 | 4% |
| 5 | F5 | 14 | 3% |
| 6 | Microsoft | 12 | 3% |
| 7 | Apache | 11 | 3% |
| 8 | WordPress | 11 | 3% |
| 9 | 深圳市腾讯计算机系统有限公司 | 10 | 2% |
| 10 | 其他 | 285 | 70% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 61 个电信行业漏洞，30 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“Tenda AC15 缓冲区溢出漏洞（CNVD-2022-75823）、Samsung Galaxy Store 输入验证错误漏洞（CNVD-2022-76491）”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/

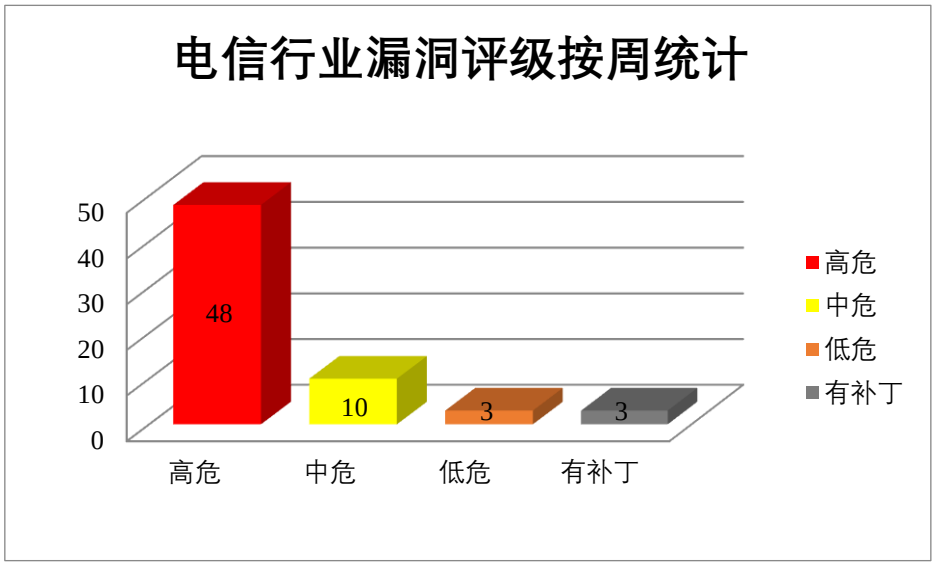


图 3 电信行业漏洞统计

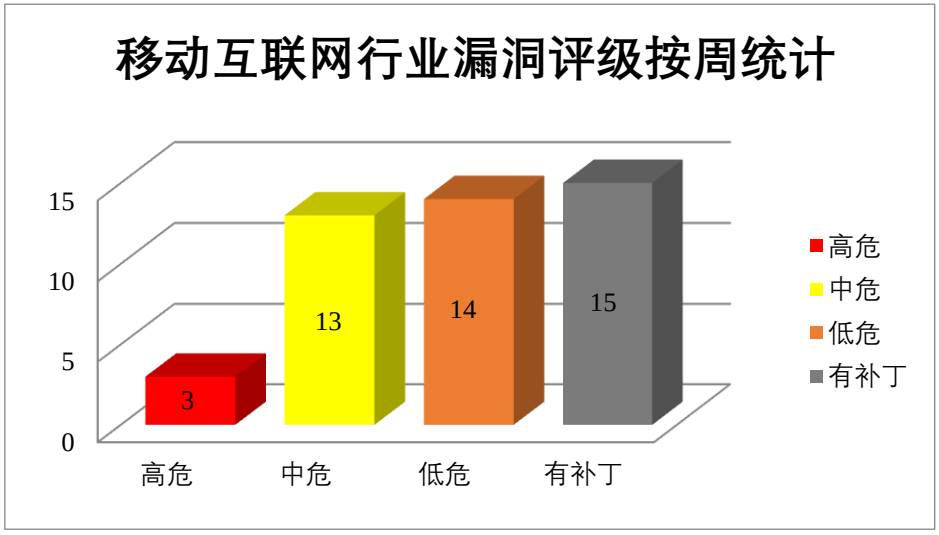


图 4 移动互联网行业漏洞统计

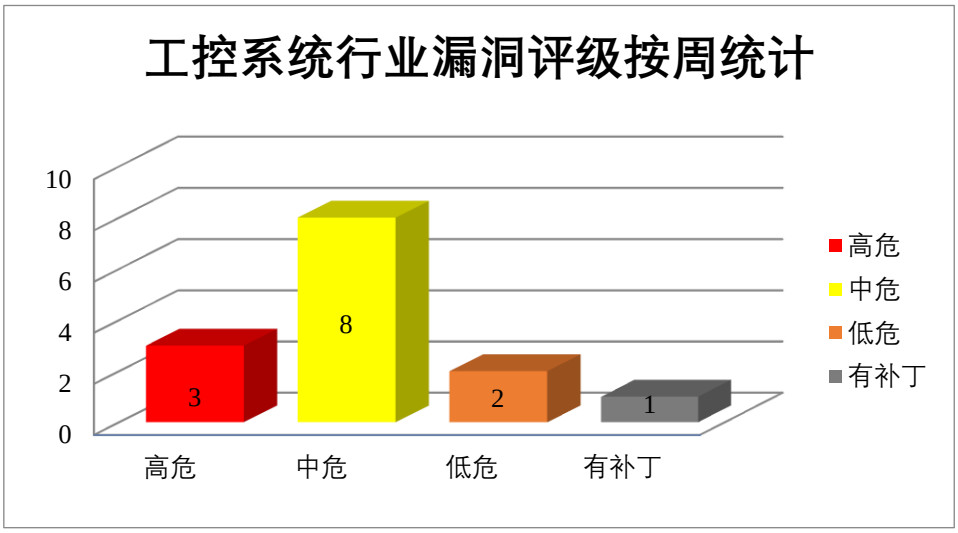


图 5 工控系统行业漏洞统计

## 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、F5 产品安全漏洞

F5 F5OS-A 是美国 F5 公司的一种操作系统软件。F5 BIG-IP 是 F5 公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。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对 Docker 注册表的只读访问权，导致服务降级，从而导致 BIG-IP 系统上的拒绝服务等。

CNVD 收录的相关漏洞包括：F5 F5OS-A 信息泄露漏洞、F5 BIG-IP 资源管理错误漏洞（CNVD-2022-74967、CNVD-2022-74965）、F5 BIG-IP 输入验证错误漏洞（CNVD-2022-74966）、F5 BIG-IP 路径遍历漏洞、F5 BIG-IP 代码问题漏洞（CNVD-2022-74968）、F5 BIG-IP iControl SOAP 目录遍历漏洞、F5 BIG-IP APM 资源管理错误漏洞（CNVD-2022-74964）。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-2022-74969

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74967

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74965

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74966

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74963

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74968

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74718

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74964

### 2、Microsoft 产品安全漏洞

Microsoft Windows SMB Server 是美国微软（Microsoft）公司的一个网络文件共享协议。它允许计算机上的应用程序读取和写入文件以及从计算机网络中的服务器程序请求服务。Microsoft Windows 是美国微软（Microsoft）公司的一种桌面操作系统。Microsoft Windows Remote Desktop Protocol（RDP）是美国微软（Microsoft）公司的一款用于连接远程 Windows 桌面的应用。Microsoft Windows Network File System 是美国微软（Microsoft）公司的一种文件共享解决方案，可让您使用 NFS 协议在运行 Windows Server 和 UNIX 操作系统的计算机之间传输文件。Microsoft Graphics Components 是美国微软（Microsoft）公司的图形驱动组件。Microsoft Dynamics 是美国微软（Microsoft）公司的一套适用于跨国企业的 ERP 业务解决方案。该产品包括财务管理、生产管理和商业智能管理等。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任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows SMB 远程代码执行漏洞（CNVD-2022-74599、CNVD-2022-74598、CNVD-2022-74596）、Microsoft Windows Server Service 远程代码执行漏洞、Microsoft Windows Remote Desktop Protocol 远程代码执行漏洞、Microsoft Windows Network File System 远程代码执行漏洞（CNVD-2022-74601）、Microsoft Windows Graphics 组件远程代码执行漏洞（CNVD-2022-74593）、Microsoft Dynamics 365 (on-premises)远程代码执行漏洞。其中，“Microsoft Windows Server Service 远程代码执行漏洞、Microsoft Windows Remote Desktop Protocol 远程代码执行漏洞、Microsoft Windows Network File System 远程代码执行漏洞（CNVD-2022-74601）、Microsoft Windows Graphics 组件远程代码执行漏洞（CNVD-2022-74593）、Microsoft Dynamics 365 (on-premises)远程代码执行漏洞”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-2022-74599
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74598
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74596
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74597
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74600
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74601
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74593
https://www.cnvd.org.cn/flaw/show/CNVD-2022-74591

### 3、 Apache 产品安全漏洞

Apache UIMA 是美国阿帕奇（Apache）基金会的一个组件化的软件架构。用于分析同终端用户相关联的大容量非结构化信息。Apache Traffic Server（ATS 或 TS）是一个高性能的、模块化的 HTTP 代理和缓存服务器，与 Nginx 和 Squid 类似。Traffic Serv

er 最初是 Inktomi 公司的商业产品，该公司在 2003 年被 Yahoo 收购，2009 年 8 月 Yaho o 向 Apache 软件基金会（ASF）贡献了源代码，并于 2010 年 4 月成为了 ASF 的顶级项目（Top-LevelProject）。 Apache TrafficServer 现在是一个开源项目，开发语言为 C++。Apache NiFi 是一套数据处理和分发系统。该系统主要用于数据路由、转换和系统中介逻辑。Apache JSPWiki 是美国阿帕奇（Apache）基金会的一款基于 Java、Servlet 和 JS P 构建的开源 WikiWiki 引擎。Apache Isis 是美国阿帕奇（Apache）基金会的一个用于在 Java 中快速开发领域驱动应用程序的框架。Apache Hadoop 是美国阿帕奇（Apache）基金会的一套开源的分布式系统基础架构。该产品能够对大量数据进行分布式处理，并具有高可靠性、高扩展性、高容错性等特点。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。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，使用精心设计的 ZIP 条目名称在指定目标目录之外创建文件，执行任意命令等。

CNVD 收录的相关漏洞包括：Apache UIMA 路径遍历漏洞、Apache Traffic Server 输入验证漏洞（CNVD-2022-76238）、Apache NiFi 存在命令执行漏洞、Apache JSPWi ki 跨站请求伪造漏洞（CNVD-2022-76239）、Apache Isis 授权问题漏洞、Apache Isis 跨站脚本漏洞、Apache Hadoop 代码问题漏洞、Apache Airflow 输入验证错误漏洞。其中，“Apache UIMA 路径遍历漏洞、Apache Traffic Server 输入验证漏洞（CNVD-202 2-76238）、Apache NiFi 存在命令执行漏洞、Apache JSPWiki 跨站请求伪造漏洞（CN VD-2022-76239）、Apache Hadoop 代码问题漏洞”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-2022-76232
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76238
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75959
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76239
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76235
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76234
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76237
https://www.cnvd.org.cn/flaw/show/CNVD-2022-76233

### 4、Siemens 产品安全漏洞

Parasolid 是一个 3D 几何建模工具，它支持多种技术，包括实体建模、直接编辑和自由曲面/表建模。JT2Go 是一个 3D JT 查看工具，允许用户查看 JT、PDF、Solid Edg e、PLM XML 以及可用的 JT、VFZ、CGM 和 TIF 数据。Teamcenter Visualization 使企业能够通过全面的可视化解决方案系列增强其产品生命周期管理 (PLM) 环境。该软件使企业用户能够在单一环境中访问文档、2D 图纸和 3D 模型。本周，上述产品被披露存

在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Parasolid 越界写入漏洞、Siemens Parasolid 越界读取漏洞、Siemens JT2Go and Teamcenter Visualization 越界写入漏洞、Siemens JT2Go and Teamcenter Visualization 越界读取漏洞（CNVD-2022-75551、CNVD-2022-75550）、Siemens JT2Go and Teamcenter Visualization 免费后使用漏洞、Siemens JT2Go and Teamcenter Visualization 缓冲区溢出漏洞（CNVD-2022-75548、CNVD-2022-75553）。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-2022-75535
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75536
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75552
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75551
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75550
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75549
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75548
https://www.cnvd.org.cn/flaw/show/CNVD-2022-75553

### 5、Tenda AC18 远程命令执行漏洞

Tenda AC18 是中国腾达（Tenda）公司的一款路由器。本周，Tenda AC18 被披露存在远程命令执行漏洞。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-2022-75821

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.htm

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-2022-75547 | 多款 Siemens 产品跨站请求伪造漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-478960.html |
| CNVD-2022-76219 | WordPress plugin Cab fare calcula 文件包含漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wpscan.com/vulnerability/680121fe-6668-4c1a-a30d-e70dd9be5aac |
| CNVD-2022-76221 | WordPress plugin Admin Word Count Column 任意文件读取漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/6293b319-dc4f-4412-9d56-55744246c99 |

| | | | |
|---|---|---|---|
| | | | 0 |
| CNVD-2022-76498 | Thales Safenet Authentication Client 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://cpl.thalesgroup.com/ |
| CNVD-2022-76508 | Samsung Account 隐式意图劫持漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6 |
| CNVD-2022-76515 | Google Chrome 资源管理错误漏洞（CNVD-2022-76515） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新:https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html |
| CNVD-2022-76513 | Google Chrome 缓冲区溢出漏洞（CNVD-2022-76513） | 高 | 目前厂商已提供补丁或者升级程序，建议使用此软件的用户随时关注厂商的主页以获取最新版本：https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html |
| CNVD-2022-76495 | Espressif ESP-IDF 内存破坏漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/espressif/esp-idf/security/advisories/GHSA-7f7f-jj2q-28wm |
| CNVD-2022-75534 | Siemens Mendix SAML Module 认证绕过漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-638652.html |
| CNVD-2022-75876 | TOTOLINK A7000R 存在命令执行漏洞（CNVD-2022-75876） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.cn/ |

小结：本周，F5 产品被披露存在多个漏洞，攻击者可利用漏洞获取对 Docker 注册表的只读访问权，导致服务降级，从而导致 BIG-IP 系统上的拒绝服务等。此外，Microsoft 、Apache、Siemens 等多款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，使用精心设计的 ZIP 条目名称在指定目标目录之外创建文件，执行任意命令等。另外，Tenda AC18 被披露存在远程命令执行漏洞。攻击者可利用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、FacturaScripts 跨站脚本漏洞（CNVD-2022-76230）

**验证描述**

FacturaScripts 是一个 ERP 软件。

FacturaScripts 2022.07 之前版本存在跨站脚本漏洞，攻击者可利用该漏洞执行任意 javascript 代码，窃取用户的 cookie，执行 HTTP 请求，获取“同源”页面内容等。

**验证信息**

POC 链接：https://huntr.dev/bounties/4578a690-73e5-4313-840c-ee15e5329741/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-76230

**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. 多个漏洞影响 OpenLiteSpeed Web 服务器软件

开源 OpenLiteSpeed Web Server 及其企业变种中发现了多个安全漏洞，这些漏洞可以被武器化以实现远程代码执行。

参考链接：https://thehackernews.com/2022/11/multiple-high-severity-flaw-affect.html

### 2. 研究人员因发现谷歌像素锁定屏幕漏洞获得 7 万美元奖励

谷歌修复了一个影响所有 Pixel 智能手机的严重安全漏洞，该漏洞可以让攻击者解锁设备。据悉该漏洞发现者获得了 7 万美元的漏洞赏金。

参考链接：https://securityaffairs.co/wordpress/138372/mobile-2/google-pixel-lock-screen-bypass.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