国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 11 月 27 日-2023 年 12 月 03 日 **2023 年第 48 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 482 个，其中高危漏洞 174 个、中危漏洞 288 个、低危漏洞 20 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 412 个（占 85%），其中互联网上出现“TomExam 跨站脚本漏洞、Alluxio 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漏洞总数 19630 个，与上周（61715 个）环比减少 68%。

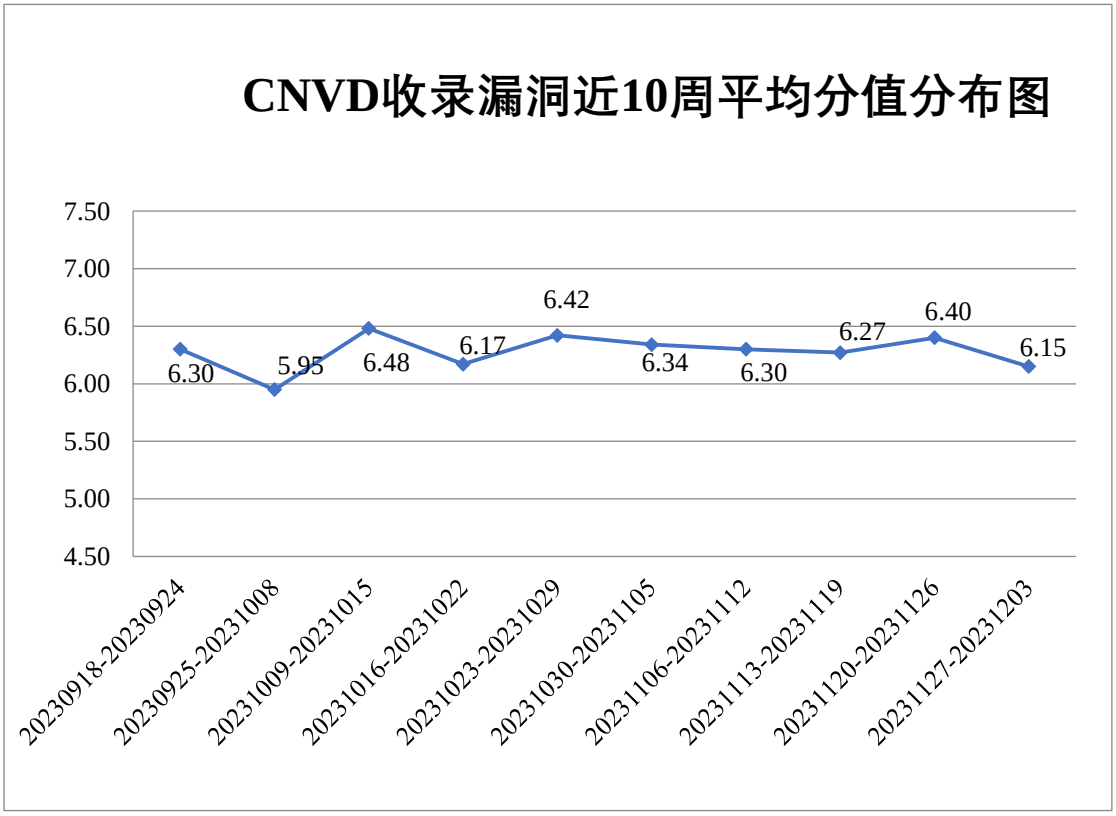

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 29 起，向基础电信企业通报漏洞事件 15 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 992 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 227 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 58 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：

智石开工业软件有限公司、郑州郑大信息技术有限公司、郑州深度软件科技有限公司、郑州大象通信信息技术有限公司、浙江宇视科技有限公司、浙江创邻科技有限公司、运城市盘石网络科技有限公司、云内控科技有限公司、钰登科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、小米科技有限责任公司、西安交大捷普网络科技有限公司、武汉天喻软件有限公司、武汉京伦科技开发有限公司、武汉金同方科技有限公司、武汉达梦数据库股份有限公司、武汉城投停车场投资建设管理有限公司、威博通科技（上海）有限公司、网是科技股份有限公司、统信软件技术有限公司、天津天堰科技股份有限公司、腾讯安全应急响应中心、太原易思软件技术有限公司、速达软件技术（广州）有限公司、四创科技有限公司、四川北斗智慧物联科技有限公司、石家庄市征红网络科技有限公司、深圳市联软科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市锟铻科技有限公司、深圳市科脉技术股份有限公司、深圳市金蝶天燕云计算股份有限公司、深圳市惠尔顿信息技术有限公司、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、深圳市必联电子有限公司、深圳市百为通达科技有限公司、深圳市昂捷信息技术股份有限公司、深圳前行智能系统有限公司、深圳极速创想科技有限公司、上海卓卓网络科技有限公司、上海甄云信息科技有限公司、上海水护盾健康科技有限公司、上海商派网络科技有限公司、上海荃路软件开发工作室、上海企望信息科技有限公司、上海穆云智能科技有限公司、上海华测导航技术股份有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海布雷德科技有限公司、上海博达数据通信有限公司、上海伯俊软件科技有限公司、商派软件有限公司、陕西小伙伴网络科技有限公司、山东领图信息科技股份有限公司、山东科德电子有限公司、厦门正航软件科技有限公司、三星（中国）投资有限公司、三菱电机株式会社、赛摩智能科技集团股份有限公司、赛蓝（广州）信息技术有限公司、瑞斯康达科技发展股份有限公司、锐捷网络股份有限公司、青岛软微网络科技有限公司、启明信息技术股份有限公司、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、普天新能源有限责任公司、明觉科技（北京）有限公司、美林数据技术股份有限公司、辽宁畅通数据通信有限公司、联想（北京）有限公司、乐跑体育互联网（武汉）有限公司、蓝网科技股份有限公司、科大讯飞股份有限公司 1、开放原子开源基金会、景腾多媒体股份

有限公司、金卡银证软件（杭州）有限公司、金富瑞（北京）科技有限公司、金蝶软件（中国）有限公司、江苏捷成睿创科技发展有限公司、佳能（中国）有限公司、佳都科技集团股份有限公司、济南宏之博信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华为云计算技术有限公司、湖南途记互联科技有限公司、湖南听风者信息科技有限公司、湖南强智科技发展有限公司、湖南麒麟信安科技股份有限公司、湖南建研信息技术股份有限公司、湖北统讯智能科技有限公司、宏脉信息技术（广州）股份有限公司、合肥六出网络科技有限公司、合肥贰道网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州荷花软件有限公司、杭州海康威视系统技术有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、杭州短链网络技术有限公司、海开智慧（北京）科技服务有限公司、广州图创计算机软件开发有限公司、广州市凝智科技有限公司、广州市科传计算机科技股份有限公司、广州酷狗计算机科技有限公司、广州恒企教育科技有限公司、广州翰智软件有限公司、广联达科技股份有限公司、广汇能源股份有限公司、广东全程云科技有限公司、广东飞企互联科技股份有限公司、福建顶点软件股份有限公司、福建博思软件股份有限公司、泛微网络科技股份有限公司、东莞市智跃软件科技有限公司、东莞市通天星软件科技有限公司、东莞谱标软件开发有限公司、鼎捷软件股份有限公司、帝国软件、大连华天软件有限公司、北京中科服科技有限公司、北京中创视讯科技有限公司、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责任公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京万户软件技术有限公司、北京思纽教育科技有限公司、北京兰德华电子技术有限公司、北京库巴扎信息科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京集翔信息技术集团有限公司、北京火星高科数字科技有限公司、北京慧舟普度科技有限公司、北京宏景世纪软件股份有限公司、北京和欣运达科技有限公司、北京格尺科技有限公司、北京高速波软件有限公司、北京邦永科技有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、百望股份有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽科迅教育装备集团有限公司、阿里巴巴集团安全应急响应中心、OpenCloudOS 开源社区和 ABB。

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、深信服科技股份有限公司、北京神州绿盟科技有限公司、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。奇安星城网络安全运营服务（长沙）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、联想集团、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、亚信科技（成都）

有限公司、安徽锋刃信息科技有限公司、贵州多彩网安科技有限公司、杭州默安科技有限公司、湖南泛联新安信息科技有限公司、内蒙古洞明科技有限公司、合肥梆梆信息科技有限公司、江西和尔惠信息技术有限公司、平安银河实验室、安徽天行网安信息安全技术有限公司、山石网科通信技术股份有限公司、贵州华黔信安信息技术有限公司、河南灵创电子科技有限公司、上海直画科技有限公司、深圳昂楷科技有限公司、广州中科诺泰技术有限公司、西安交大捷普网络科技有限公司、江苏极元信息技术有限公司、苏州棱镜七彩信息科技有限公司、北京威努特技术有限公司、北京天防安全科技有限公司、北京众安天下科技有限公司、江苏金陵科技集团有限公司、成都安美勤信息技术股份有限公司、北京时代新威信息技术有限公司、杭州智顺科技有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 19630 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奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 17610 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
奇安信网神（补天平台）	9430	9430
斗象科技（漏洞盒子）	8003	8003
北京天融信网络安全技术有限公司	994	10
深信服科技股份有限公司	923	0
北京神州绿盟科技有限公司	631	255
北京数字观星科技有限公司	429	0
安天科技集团股份有限公司	419	0
新华三技术有限公司	336	0
杭州迪普科技股份有限公司	228	209
三六零数字安全科技集团有限公司	177	177
阿里云计算有限公司	156	5
北京启明星辰信息安全技术有限公司	136	56

杭州安恒信息技术股份有限公司	73	0
北京长亭科技有限公司	61	1
北京升鑫网络科技有限公司（青藤云）	42	42
中电科网络安全科技股份有限公司	27	11
中国电信股份有限公司网络安全产品运营中心	3	3
北京智游网安科技有限公司	2	2
北京安信天行科技有限公司	2	2
南京联成科技发展股份有限公司	1	1
北京知道创宇信息技术有限公司	1	0
奇安星城网络安全运营服务（长沙）有限公司	87	87
河南东方云盾信息技术有限公司	54	54
快页信息技术有限公司	47	47
联想集团	42	42
江苏金盾检测技术股份有限公司	34	34
北京山石网科信息技术有限公司	30	30
亚信科技（成都）有限公司	28	28
安徽锋刃信息科技有限公司	18	18

贵州多彩网安科技有限公司	16	16
杭州默安科技有限公司	9	9
湖南泛联新安信息科技有限公司	8	8
内蒙古洞明科技有限公司	6	6
合肥梆梆信息科技有限公司	6	6
江西和尔惠信息技术有限公司	5	5
平安银河实验室	3	3
安徽天行网安信息安全技术有限公司	3	3
山石网科通信技术股份有限公司	3	3
贵州华黔信安信息技术有限公司	3	3
河南灵创电子科技有限公司	2	2
上海直画科技有限公司	2	2
深圳昂楷科技有限公司	2	2
广州中科诺泰技术有限公司	2	2
西安交大捷普网络科技有限公司	1	1
江苏极元信息技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
北京威努特技术有限公司	1	1

北京天防安全科技有限公司	1	1
北京众安天下科技有限公司	1	1
江苏金陵科技集团有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
北京时代新威信息技术有限公司	1	1
杭州智顺科技有限公司	1	1
任子行网络技术股份有限公司	1	1
CNCERT 河北分中心	3	3
CNCERT 广西分中心	1	1
个人	998	998
报送总计	23497	19630

本周漏洞按类型和厂商统计

本周，CNVD 收录了 482 个漏洞。WEB 应用 220 个，应用程序 136 个，网络设备（交换机、路由器等网络端设备）85 个，智能设备（物联网终端设备）18 个，安全产品 12 个，操作系统 5 个，车联网 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	220
应用程序	136
网络设备（交换机、路由器等网络端设备）	85
智能设备（物联网终端设备）	18
安全产品	12
操作系统	5
车联网	4
数据库	2

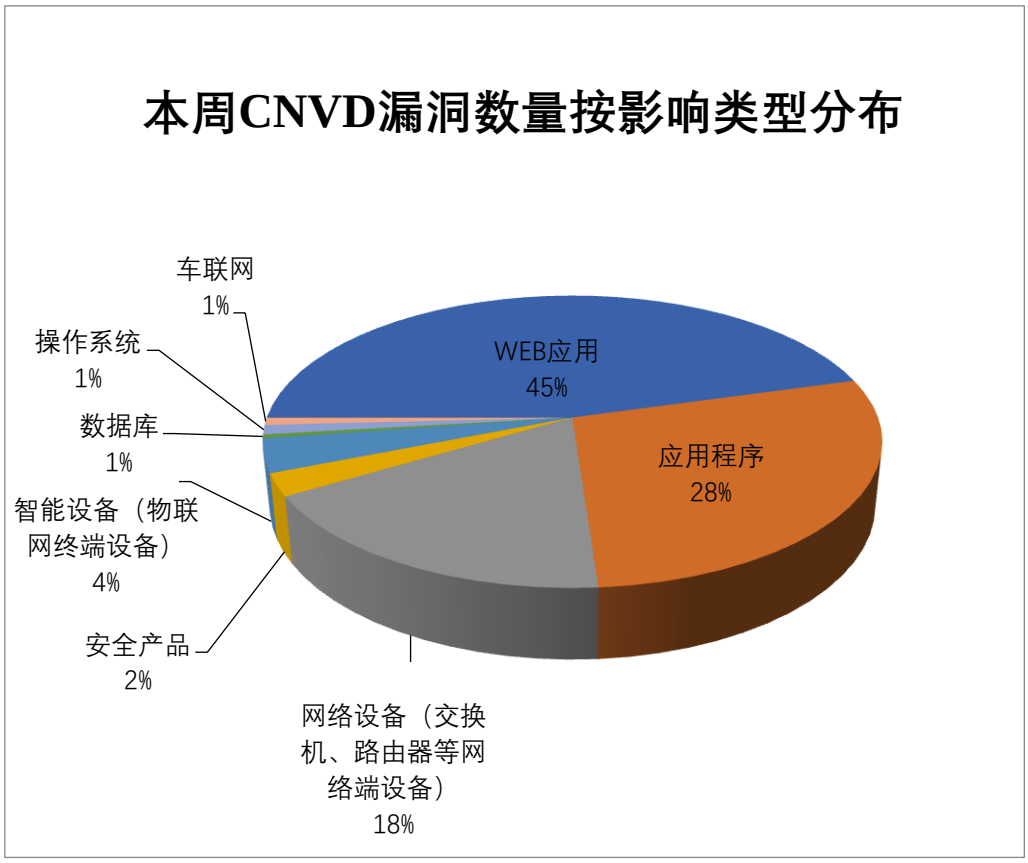

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Cisco、Apache 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	32	7%
2	Cisco	24	5%
3	Apache	11	2%
4	Microsoft	11	2%
5	用友网络科技股份有限公司	11	2%
6	浙江大华技术股份有限公司	9	2%
7	北京百卓网络技术有限公司	8	2%
8	普联技术有限公司	8	2%
9	bloofoxCMS	7	1%
10	其他	361	75%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，33 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，“Apple iOS 和 iPadOS 缓冲区溢出漏洞、AVEVA InTouch 命令注入漏洞”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/

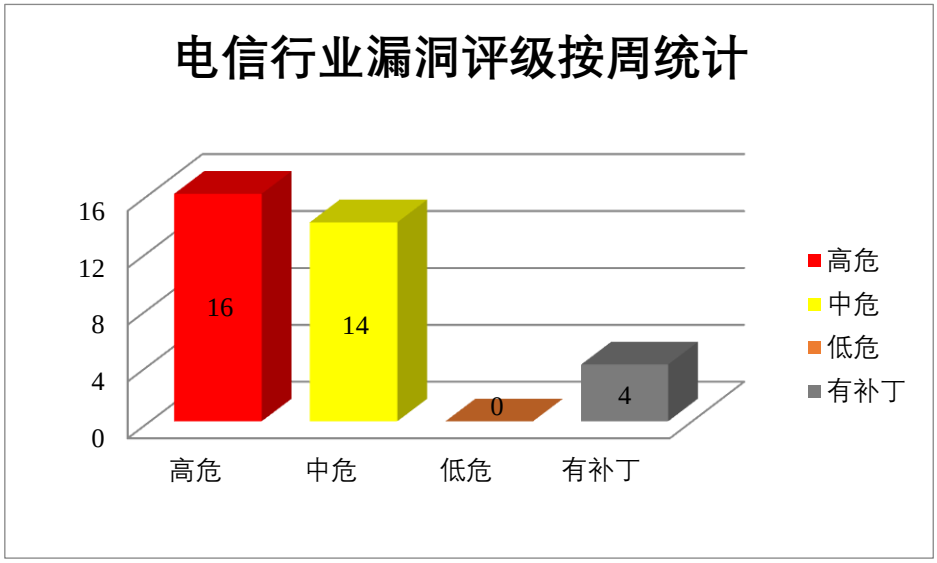

图 3 电信行业漏洞统计

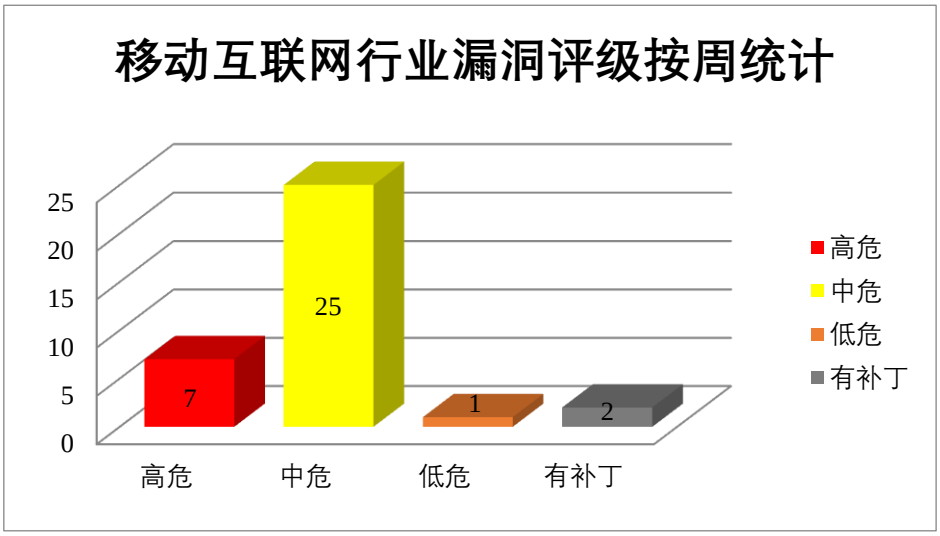

图 4 移动互联网行业漏洞统计

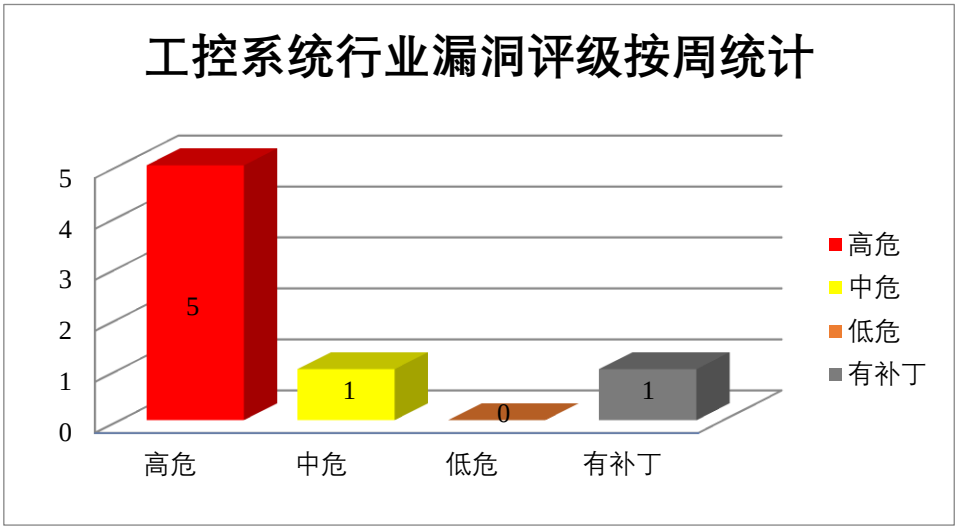

图 5 工控系统行业漏洞统计

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 After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。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用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe After Effects 越界读取漏洞（CNVD-2023-91788、CNVD-2023-91794、CNVD-2023-91793、CNVD-2023-91791）、Adobe After Effects 越界写入漏洞（CNVD-2023-91787、CNVD-2023-91790）、Adobe ColdFusion 代码执行漏洞（CNVD-2023-94489、CNVD-2023-94490）。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-2023-91788

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91787

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91791

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91790

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91794

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91793

https://www.cnvd.org.cn/flaw/show/CNVD-2023-94489

https://www.cnvd.org.cn/flaw/show/CNVD-2023-94490

2、 Microsoft 产品安全漏洞

Microsoft Skype for Business Server 是美国微软（Microsoft）公司的一套安全统一的通信平台，它提供即时消息(IM)、音频和视频通话、联机会议、联机状态信息和共享功能。Microsoft QUIC 是美国微软（Microsoft）公司的一个网络传输协议。Microsoft Outlook 是美国微软（Microsoft）公司的一套电子邮件应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以更高的权限获取敏感信息，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Skype for Business 远程代码执行漏洞（CNVD-2023-92199、CNVD-2023-92200、CNVD-2023-92203）、Microsoft Skype for Business 权限提升漏洞（CNVD-2023-92201）、Microsoft QUIC 拒绝服务漏洞（CNVD-2023-92204、CNVD-2023-92205）、Microsoft Outlook 欺骗漏洞、Microsoft Outlook 远程代码执行漏洞（CNVD-2023-92208）。其中，除“Microsoft Skype for Business 权限提升漏洞（CNVD-2023-92201）”外，其余的综合评级为“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-2023-92199
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92200
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92201
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92203
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92204
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92205
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92207
https://www.cnvd.org.cn/flaw/show/CNVD-2023-92208

3、 Cisco 产品安全漏洞

Cisco AppDynamics PHP Agent 是美国思科（Cisco）公司的一个代理程序，用于监控 PHP 应用程序的性能。Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实施相应策略来监管网络。Cisco Unified Contact Center Express（Unified CCX）是美国思科（Cisco）公司的一款统一通信解决方案中的客户关系管理组件。该组件支持自助语音服务、呼叫分配和客户访问控制等功能。Cisco Intersight 是美国思科（Cisco）公司的一个应用平台。提供了智能管理级别，使 IT 组织能够以比前几代工具更先进的方式分析、简化和自动化其环境。Cisco SD-WAN vManage 是美国思科（Cisco）公司的一个高度可定制的仪表板。可简化和自动化 Cisco SD-WAN 的部署、配置、管理和操作。Cisco Webex Meetings 是美国思科（Cisco）公司的一套视频会议解决方案。Cisco Duo 是美国思科（Cisco）公司的一个完全托管的解决方案。提供对您

的应用程序和数据的安全访问。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞替换文件并访问敏感的服务器端信息，使用 root 权限执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco AppDynamics PHP Agent 权限提升漏洞、Cisco Identity Services Engine 任意文件写入漏洞、Cisco Unified Contact Center Express 输入验证错误漏洞（CNVD-2023-93334）、Cisco Intersight Private Virtual Appliance 命令注入漏洞、Cisco SD-WAN vManage 存在访问控制错误漏洞、Cisco Webex Meetings 任意文件上传漏洞、Cisco Identity Services Engine 命令注入漏洞（CNVD-2023-93336）、Cisco Duo 身份验证错误漏洞。其中，“Cisco Identity Services Engine 任意文件写入漏洞、Cisco Intersight Private Virtual Appliance 命令注入漏洞、Cisco Duo 身份验证错误漏洞”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-2023-93325

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93327

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93334

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93333

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93331

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93337

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93336

https://www.cnvd.org.cn/flaw/show/CNVD-2023-93335

4、Apache 产品安全漏洞

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 Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。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 OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache Jena 是美国阿帕奇（Apache）基金会的一个 Java 语义网框架。用于构建语义 Web 和链接数据应用程序。Apache InLong 是美国阿帕奇（Apache）基金会的一站式的海量数据集成框架。提供自动化、安全、可靠的数据传输能力。Apache ActiveMQ 是美国阿帕奇（Apache）基金会的一套开源的消息中间件，它支持 Java 消息服务、集群、Spring Framework 等。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身份验证绕过，通过 SPARQL 查询执行任意 javascript 导致拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Airflow 授权问题漏洞（CNVD-2023-93318）、Apache Traffic Server 输入验证错误漏洞（CNVD-2023-93321）、Apache HTTP Server 缓冲区溢出漏洞（CNVD-2023-93320）、Apache OFBiz 访问控制错误漏洞、Apache Je

na 跨站脚本漏洞、Apache InLong 反序列化漏洞（CNVD-2023-93323）、Apache Traffic Server 信息泄露漏洞（CNVD-2023-93322）、Apache ActiveMQ 反序列化漏洞。除“Apache Airflow 授权问题漏洞（CNVD-2023-93318）、Apache OFBiz 访问控制错误漏洞、Apache Jena 跨站脚本漏洞”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-2023-93318
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93321
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93320
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93319
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93324
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93323
https://www.cnvd.org.cn/flaw/show/CNVD-2023-93322
https://www.cnvd.org.cn/flaw/show/CNVD-2023-94073

5、baserCMS 代码注入漏洞

baserCMS 是 baserCMS 团队的一套企业级内容管理系统（CMS）。本周，baserCMS 被披露存在代码注入漏洞。攻击者可利用该漏洞通过 mail form 注入代码。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-2023-93330

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-2023-94075	CasaOS 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/IceWhaleTech/CasaOS/commit/d060968b7ab08e7f8cbfe7ca9ccdfa47afe9bb06
CNVD-2023-94706	AVEVA InTouch 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec126.pdf
CNVD-2023-94705	Apple iOS 和 iPadOS 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：https://support.apple.com/en-us/HT213346

CNVD-2023-91788	Adobe After Effects 越界读取漏洞（CNVD-2023-91788）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/after_effects/apsb23-66.html
CNVD-2023-92199	Microsoft Skype for Business 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36786
CNVD-2023-92204	Microsoft QUIC 拒绝服务漏洞	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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36435
CNVD-2023-92208	Microsoft Outlook 远程代码执行漏洞（CNVD-2023-92208）	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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895
CNVD-2023-93320	Apache HTTP Server 缓冲区溢出漏洞（CNVD-2023-93320）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://httpd.apache.org/security/vulnerabilities_24.html
CNVD-2023-93327	Cisco Identity Services Engine 任意文件写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR
CNVD-2023-93335	Cisco Duo 身份验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-mac-bypass-OyZpVPnx

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，Microsoft、Cisco、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞以更高的权限获取敏感信息，在系统上执行任意代码，导致身份验证绕过，通过 SPARQL 查询执行任意 javascript 导致拒绝服务等。另外，baserCMS 被披露存在代码注入漏洞。攻击者可利用漏洞通过 mail form 注入代码。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、TomExam 跨站脚本漏洞

验证描述

TomExam 是一款免费高效的网络考试系统软件。

TomExam 3.0 版本存在跨站脚本（XSS）漏洞，攻击者可利用该漏洞通过 p_name 参数传递给 list.thtml，导致跨站脚本(XSS)。

验证信息

POC 链接：https://www.cnblogs.com/mrhonest/p/16949304.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-93550

信息提供者

深信服科技股份有限公司

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. 谷歌从 12 月开始删除不活跃时间逾两年的账号

从 12 月 1 日开始，Google 将对账号进行大清洗。今年五月搜索巨人通过官方博客宣布从 12 月 1 日起永久删除超过两年时间不活跃/不登陆的账号。Google 表示此举旨在防止遗弃的账号被入侵后用于发送垃圾邮件。

参考链接：https://arstechnica.com/gadgets/2023/11/inactive-google-account-deletions-start-december-1/

2. Windows 用户报告系统上突然安装了惠普打印机软件

Windows 用户报告系统上突然安装了惠普打印机软件，而他们的机器并没有连接任何惠普公司的设备。

参考链接：https://www.theregister.com/2023/11/30/windows_hp_software_uninvited/

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