国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 12 月 25 日-2023 年 12 月 31 日 **2023 年第 52 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 407 个，其中高危漏洞 132 个、中危漏洞 251 个、低危漏洞 24 个。漏洞平均分值为 6.06。本周收录的漏洞中，涉及 0day 漏洞 245 个（占 60%），其中互联网上出现“WordPress 插件 Frontend File Manager 安全绕过漏洞、WordPress 插件 Coming Soon Page & Maintenance Mode 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 109390 个，与上周（78107 个）环比增加 40%。

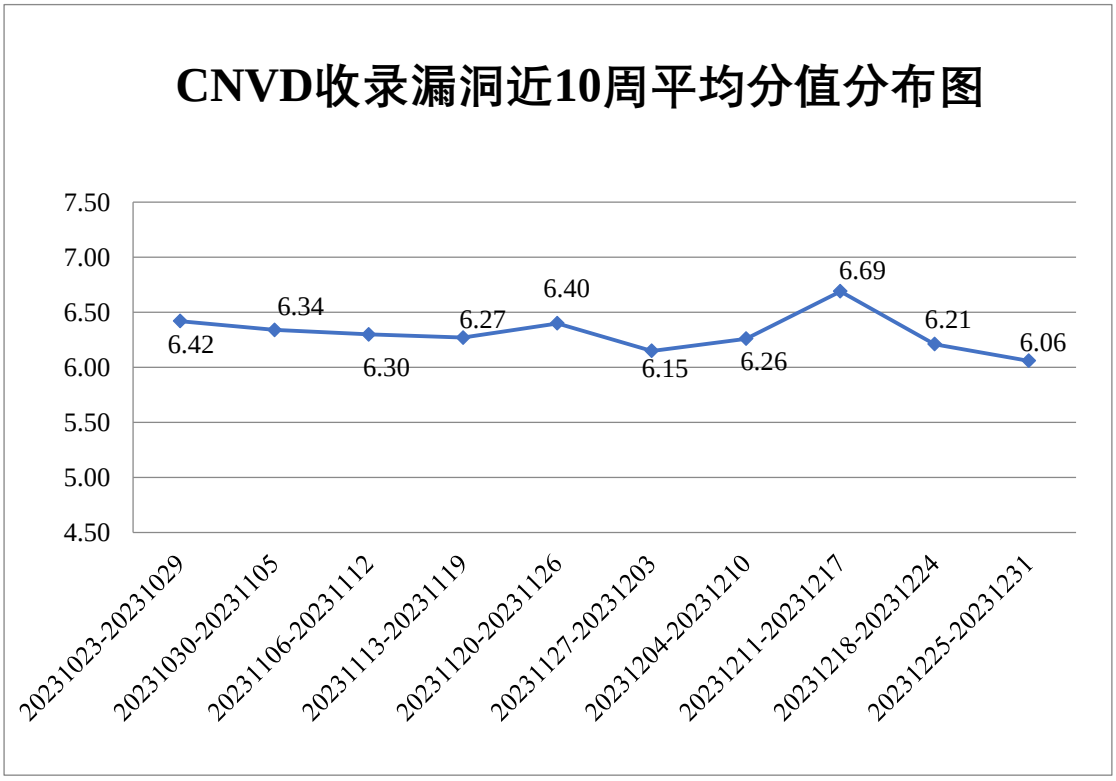

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 11 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 967 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 243 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 27 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：

紫光软件系统有限公司、猪八戒股份有限公司、珠海奔图打印科技有限公司、重庆猫扑网络科技有限公司、中控泰科（北京）科技发展有限公司、中孚信息股份有限公司、浙江宇视科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、西门子（中国）有限公司、西安大西信息科技有限公司、天津百望金赋科技有限公司、苏州科达科技股份有限公司、松立控股集团股份有限公司、四川五洲智慧城科技有限公司、四川思途智旅软件有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、深圳维盟科技股份有限公司、深圳市中科网威科技有限公司、深圳市新泊乐停车技术有限公司、深圳市想播就播科技有限公司、深圳市联新移动医疗科技有限公司、深圳市锟铻科技有限公司、深圳市方直科技股份有限公司、深圳市鼎禾盛食品科技有限公司、深圳市顶讯网络科技有限公司、深圳市昂捷信息技术股份有限公司、深圳华锐分布式技术股份有限公司、上海兴容信息技术有限公司、上海西岸科创企业发展有限公司、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、上海艾泰科技有限公司、山东欧倍尔软件科技有限责任公司、青岛自动化仪表有限公司、青岛智链顺达科技有限公司、南京毅成达信息技术有限公司、南京帆软软件有限公司、朗坤智慧科技股份有限公司、蓝网科技股份有限公司、江苏天瑞仪器股份有限公司、吉翁电子（深圳）有限公司、湖南强智科技发展有限公司、杭州思福迪信息技术有限公司、杭州趣链科技有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、杭州白书科技有限公司、广州盈可视电子科技有限公司、广州图创计算机软件开发有限公司、广州拓波软件科技有限公司、广州市成格信息技术有限公司、广西南宁领众网络科技有限公司、广东伟达智能装备股份有限公司、广东天琴信息技术有限公司、帆软软件有限公司、东方希望集团有限公司、鼎捷软件股份有限公司、诚天国际供应链（深圳）有限公司、成都任我行软件股份有限公司、毕孚自动化设备贸易（上海）有限公司、北京中软国际教育科技股份有限公司、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、北京心领育科技有限公司、北京沃丰时代数据科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京派网软件有限公司、北京龙软科技股份有限公司、北京朗新天霁软件技术有限公司、北京九思协同软件有限公司、北京构力科技有限公司、北京佰才邦技术股份有限公司、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、安徽旭帆信息科技有限公司、爱普生（中国）有限公司和 WAVLINK。

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、北京神州绿盟科技有限公司、深信服科技股份有限公司、北京数字观星科技有限公司、天津市国瑞数码安全系统股份有限公司等单位报送公开收集的漏洞数量较多。博智安全科技股份有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、中孚安全技术有限公司、内蒙古洞明科技有限公司、贵州多彩网安科技有限公司、北京山石网科信息技术有限公司、联想集团、亚信科技（成都）有限公司、湖南泛联新安信息科技有限公司、北京远禾科技有限公司、北京卓识网安技术股份有限公司、安徽锋刃信息科技有限公司、北京天防安全科技有限公司、北京中睿天下信息技术有限公司、杭州默安科技有限公司、上海谋乐网络科技有限公司、赛尔网络有限公司、南京聚铭网络科技有限公司、江苏云天网络安全技术有限公司、江苏百达智慧网络科技有限公司（含光实验室）、杭州智顺科技有限公司、杭州安信检测技术有限公司、杭州弘沿科技有限公司、北京墨云科技有限公司、成都卓越华安信息技术服务有限公司、山东新潮信息技术有限公司、江苏君立华域信息安全技术股份有限公司、安徽天行网安信息安全技术有限公司、河南灵创电子科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、江苏极元信息技术有限公司、浙江东安检测技术有限公司、浙江安腾信息技术有限公司、上海直画科技有限公司、合肥梆梆信息科技有限公司、异图（上海）科技有限责任公司、广西网信信息技术有限公司、成都安美勤信息技术股份有限公司、北京中关村实验室、北京科技大学、南京深安科技有限公司、信息产业信息安全测评中心、江苏天竞云合数据技术有限公司、广州安海信息安全技术有限公司、济南时代确信信息安全测评有限公司、河南悦海数安科技有限公司、西藏熙安信息技术有限责任公司、墨菲未来科技（北京）有限公司及其他个人白帽子向 CNVD 提交了 109390 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 107335 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）	101527	101527
奇安信网神（补天平台）	5187	5187
北京启明星辰信息安全技术有限公司	648	27

上海交大	621	621
北京神州绿盟科技有限公司	551	0
深信服科技股份有限公司	373	2
北京数字观星科技有限公司	354	0
天津市国瑞数码安全系统股份有限公司	345	0
新华三技术有限公司	330	0
安天科技集团股份有限公司	243	0
阿里云计算有限公司	158	6
北京知道创宇信息技术有限公司	126	0
杭州安恒信息技术股份有限公司	117	1
远江盛邦（北京）网络安全科技股份有限公司	45	45
中国电信集团系统集成有限责任公司	14	1
北京天融信网络安全技术有限公司	12	12
杭州迪普科技股份有限公司	10	0
中电科网络安全科技股份有限公司	4	4
北京长亭科技有限公司	4	4
北京安信天行科技有限公司	3	3
北京智游网安科技有限公司	2	2
博智安全科技股份有	110	110

限公司		
河南东方云盾信息技术有限公司	95	95
快页信息技术有限公司	43	43
中孚安全技术有限公司	42	42
内蒙古洞明科技有限公司	38	38
贵州多彩网安科技有限公司	30	30
北京山石网科信息技术有限公司	26	26
联想集团	20	20
亚信科技（成都）有限公司	15	15
湖南泛联新安信息科技有限公司	11	11
北京远禾科技有限公司	10	10
北京卓识网安技术股份有限公司	8	8
安徽锋刃信息科技有限公司	5	5
北京天防安全科技有限公司	5	5
北京中睿天下信息技术有限公司	4	4
杭州默安科技有限公司	3	3
上海谋乐网络科技有限公司	3	3
赛尔网络有限公司	2	2
南京聚铭网络科技有限公司	2	2

江苏云天网络安全技术有限公司	2	2
江苏百达智慧网络科技有限公司（含光实验室）	2	2
杭州智顺科技有限公司	2	2
杭州安信检测技术有限公司	2	2
杭州弘沿科技有限公司	2	2
北京墨云科技有限公司	2	2
成都卓越华安信息技术服务有限公司	2	2
山东新潮信息技术有限公司	2	2
江苏君立华域信息安全技术股份有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
河南灵创电子科技有限公司	1	1
奇安星城网络安全运营服务（长沙）有限公司	1	1
江苏极元信息技术有限公司	1	1
浙江东安检测技术有限公司	1	1
浙江安腾信息技术有限公司	1	1
上海直画科技有限公司	1	1
合肥梆梆信息科技有	1	1

限公司		
异图（上海）科技有限责任公司	1	1
广西网信信息技术有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
北京中关村实验室	1	1
北京科技大学	1	1
南京深安科技有限公司	1	1
信息产业信息安全测评中心	1	1
江苏天竞云合数据技术有限公司	1	1
广州安海信息安全技术有限公司	1	1
济南时代确信信息安全测评有限公司	1	1
河南悦海数安科技有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
墨菲未来科技（北京）有限公司	1	1
CNCERT 河北分中心	6	6
CNCERT 内蒙古分中心	4	4
CNCERT 浙江分中心	1	1
个人	1425	1425
报送总计	112622	109390

本周漏洞按类型和厂商统计

本周，CNVD 收录了 407 个漏洞。应用程序 167 个，WEB 应用 166 个，网络设备

（交换机、路由器等网络端设备）35 个，操作系统 28 个，数据库 8 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
应用程序	167
WEB 应用	166
网络设备（交换机、路由器等网络端设备）	35
操作系统	28
数据库	8
智能设备（物联网终端设备）	2
安全产品	1

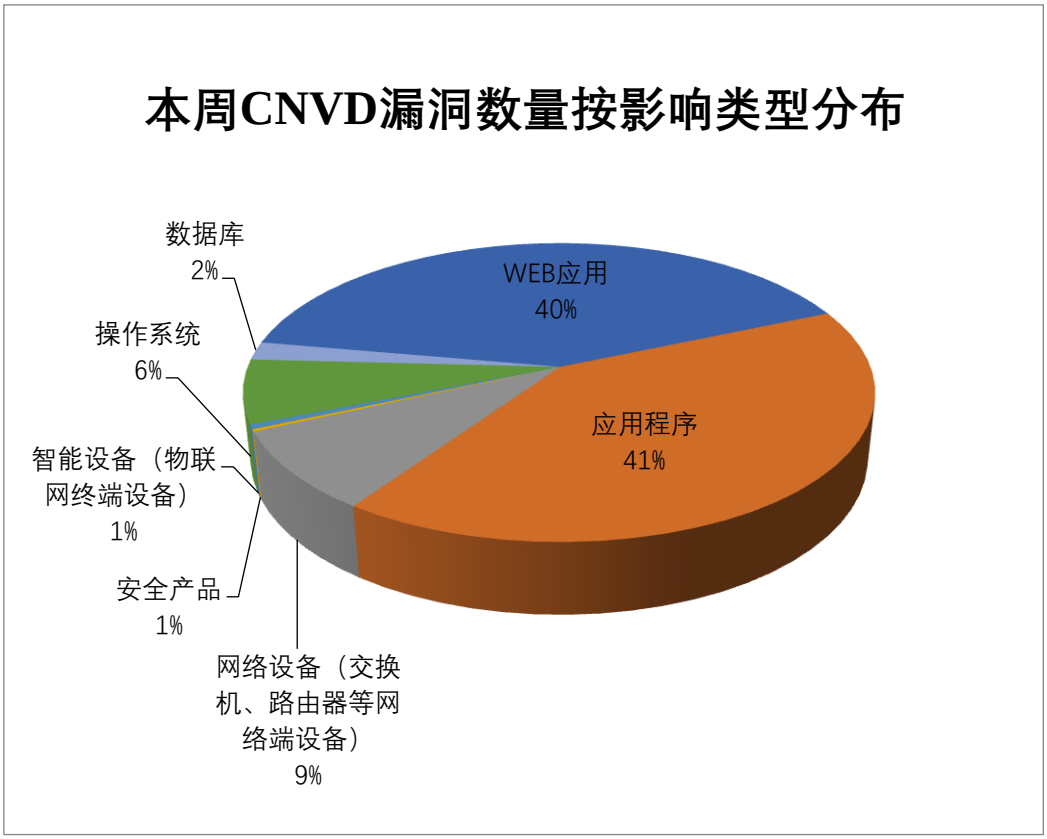

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、IBM、Google 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	88	22%
2	IBM	21	5%
3	Google	21	5%

4	SAP	10	2%
5	Microsoft	8	2%
6	WordPress	8	2%
7	北京星网锐捷网络技术有限公司	8	2%
8	Apache	7	2%
9	用友网络科技股份有限公司	6	1%
10	其他	230	57%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，36 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“IBM DB2 拒绝服务漏洞（CNVD-2023-100317）”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/

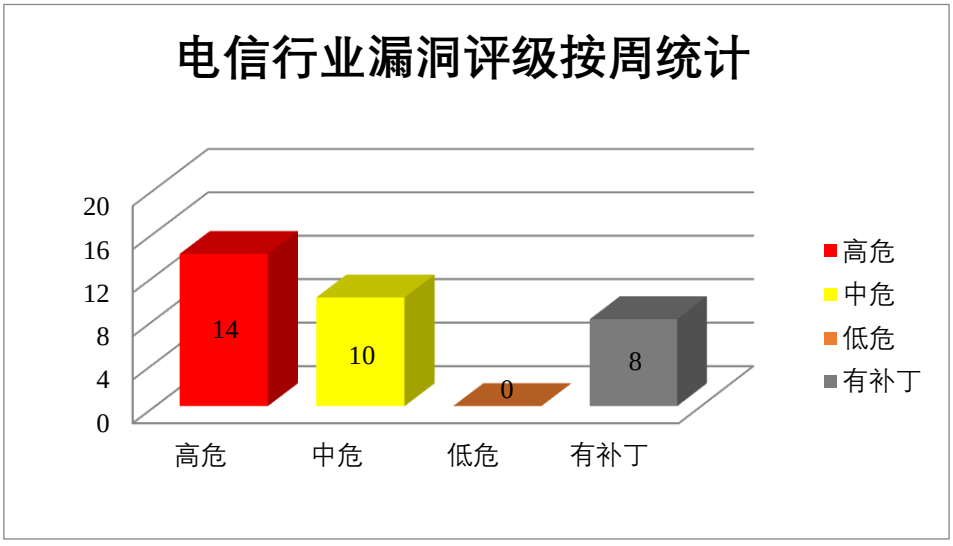

图 3 电信行业漏洞统计

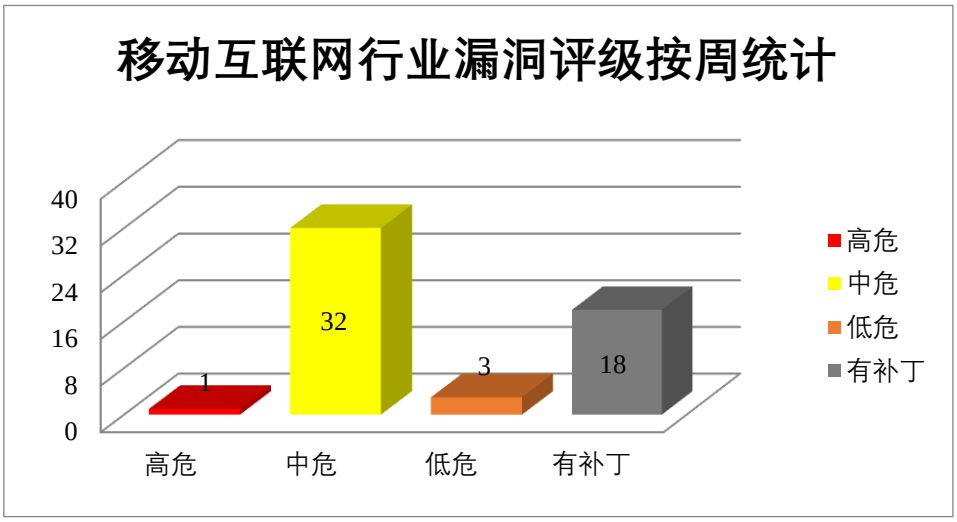

图 4 移动互联网行业漏洞统计

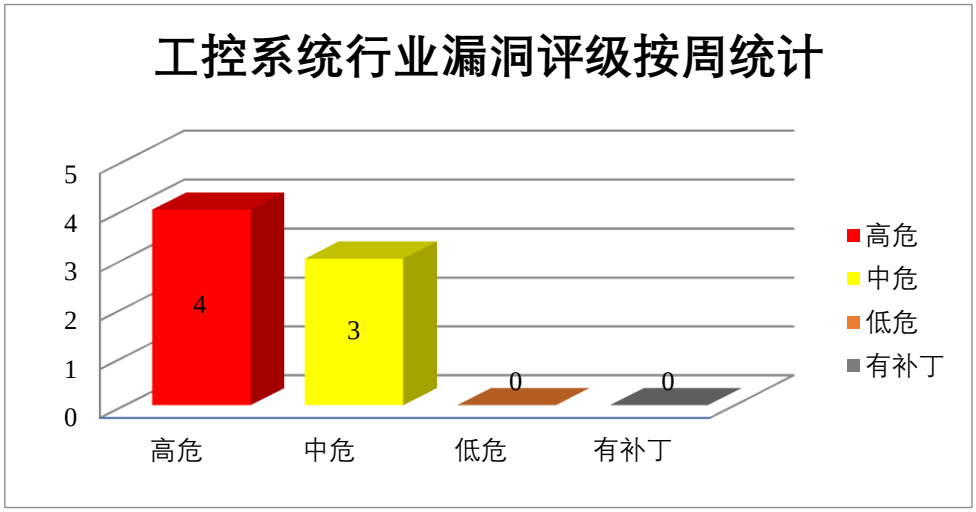

图 5 工控系统行业漏洞统计

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。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，导致权限提升。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2023-101640、CNVD-2023-101642、CNVD-2023-101645、CNVD-2023-101648、CNVD-2023-101649、CNVD-2023-101650、CNVD-2023-101651）、Google Android 权限提升漏洞（CNVD-2023-100964）。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-2023-101640

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101642

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101645

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101648

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101649

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101650

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101651

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100964

2、 Adobe 产品安全漏洞

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。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 Media Encoder 是美国奥多比（Adobe）公司的一款音、视频编码应用程序。Adobe Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。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，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：Adobe ColdFusion 路径遍历漏洞（CNVD-2023-100303）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2023-100304）、Adobe Media Encoder 越界读取漏洞（CNVD-2023-100306）、Adobe Media Encoder 堆缓冲区溢出漏洞、Adobe Dimension 越界读取漏洞（CNVD-2023-100308）、Adobe ColdFusion 访问控制错误漏洞、Adobe ColdFusion 代码执行漏洞（CNVD-2023-100310）、Adobe ColdFusion 跨站脚本漏洞（CNVD-2023-100311）。其中，“Adobe Media Encoder 越界读取漏洞（CNVD-2023-100306）、Adobe Media Encoder 堆缓冲区溢出漏洞、Adobe ColdFusion 访问控制错误漏洞、Adobe ColdFusion 代码执行漏洞（CNVD-2023-100310）”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-2023-100303

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100304

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100306

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100307

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100308

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100309

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100310

https://www.cnvd.org.cn/flaw/show/CNVD-2023-100311

3、 IBM 产品安全漏洞

IBM DB2 是美国国际商业机器（IBM）公司的一套关系型数据库管理系统。该系

统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞导致拒绝服务。

CNVD 收录的相关漏洞包括：IBM DB2 拒绝服务漏洞（CNVD-2023-100313、CNVD-2023-100314、CNVD-2023-100315、CNVD-2023-100316、CNVD-2023-100317、CNVD-2023-100318、CNVD-2023-100319、CNVD-2023-100320）。其中，“IBM DB2 拒绝服务漏洞（CNVD-2023-100317）”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-2023-100313
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100314
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100315
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100316
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100317
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100318
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100319
https://www.cnvd.org.cn/flaw/show/CNVD-2023-100320

4、 Microsoft 产品安全漏洞

Microsoft Dynamics 365 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。Microsoft Visual Studio 是美国微软（Microsoft）公司的一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃取受害者基于 cookie 的身份验证凭据，获取敏感信息，进行欺骗攻击，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Dynamics 365(on-premises)跨站脚本漏洞（CNVD-2023-101676）、Microsoft Visual Studio 信息泄露漏洞（CNVD-2023-101682）、Microsoft Visual Studio 权限提升漏洞（CNVD-2023-101683、CNVD-2023-101685、CNVD-2023-101686）、Microsoft Visual Studio 拒绝服务漏洞、Microsoft Visual Studio 远程代码执行漏洞（CNVD-2023-101687）、Microsoft Dynamics 365 Sales 欺骗漏洞。其中，“Microsoft Visual Studio 远程代码执行漏洞（CNVD-2023-101687）”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-2023-101676
https://www.cnvd.org.cn/flaw/show/CNVD-2023-101682
https://www.cnvd.org.cn/flaw/show/CNVD-2023-101683
https://www.cnvd.org.cn/flaw/show/CNVD-2023-101684

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101685

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101686

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101687

https://www.cnvd.org.cn/flaw/show/CNVD-2023-101672

5、Geeklog 跨站脚本漏洞

Geeklog 是一种开源软件，可用作 Weblog，CMS 或 Web Portal。本周，Geeklog 被披露存在跨站脚本漏洞。该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过精心设计的有效负载注入邮件设置（backend、host、port、auth）来执行任意 Web 脚本或 HTML。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-2023-101447

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-2023-100010	SAP PowerDesigner 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
CNVD-2023-100008	SAP Business One 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://me.sap.com/notes/3355658
CNVD-2023-100012	SAP NetWeaver ABAP Server 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
CNVD-2023-100014	SAP PowerDesigner 内存破坏漏洞	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
CNVD-2023-100155	IBM AIX and VIOS 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.ibm.com/support/pages/node/7095022
CNVD-2023-100307	Adobe Media Encoder 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html
CNVD-2023-100309	Adobe ColdFusion 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html
CNVD-2023-101093	Fortinet FortiPortal 命令注入漏洞	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://www.fortiguard.com/psirt/FG-IR-23-425
CNVD-2023-101127	Apache Submarine SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/g99h773vd49n1wyghdq1llv2f83w1b3r
CNVD-2023-101687	Microsoft Visual Studio 远程代码执行漏洞（CNVD-2023-101687）	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-2023-23381

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，导致权限提升。此外，Adobe、IBM、Microsoft 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，窃取受害者基于 cookie 的身份验证凭据，获取敏感信息，进行欺骗攻击，在系统上执行任意代码，导致拒绝服务等。另外，Geeklog 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过精心设计的有效负载注入邮件设置（backend、host、port、auth）来执行任意 Web 脚本或 HTML。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、WordPress 插件 Coming Soon Page & Maintenance Mode 跨站脚本漏洞

验证描述

WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress 插件 Coming Soon Page & Maintenance Mode 存在跨站脚本漏洞，攻击者可利用该漏洞窃取受害者基于 cookie 的身份验证凭据。

验证信息

POC 链接：https://blog.nintechnet.com/unauthenticated-stored-xss-in-wordpress-coming-soon-page-and-maintenance-mode-plugin/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-101688

信息提供者

北京长亭科技有限公司

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. Apache OfBiz ERP 系统中的安全漏洞使企业面临攻击

在 Apache OfBiz 中发现了一个新的零日安全漏洞，Apache OfBiz 是一个开源企业资源规划 （ERP）系统，可被利用来绕过身份验证保护。

参考链接：https://thehackernews.com/2023/12/critical-zero-day-in-apache-ofbiz-erp.html

2. Linux SSH 服务器受到攻击后被用于加密货币挖掘

威胁行为者在服务器上安装端口扫描器和字典攻击工具，目的是针对其他脆弱的服务器，并将它们纳入网络中，以进行加密货币挖矿和分布式拒绝服务（DDoS）攻击。

参考链接：https://thehackernews.com/2023/12/warning-poorly-secured-linux-ssh.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