国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 12 月 12 日-2022 年 12 月 18 日 **2022 年第 50 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 547 个，其中高危漏洞 261 个、中危漏洞 253 个、低危漏洞 33 个。漏洞平均分值为 6.52。本周收录的漏洞中，涉及 0day 漏洞 259 个（占 47%），其中互联网上出现“TOTOLINK NR1800X setOpModeCfg 缓冲区溢出漏洞、ZKTeco ZKBioSecurity SQL 注入漏洞”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 26350 个，与上周（5742 个）环比增加 3.6 倍。

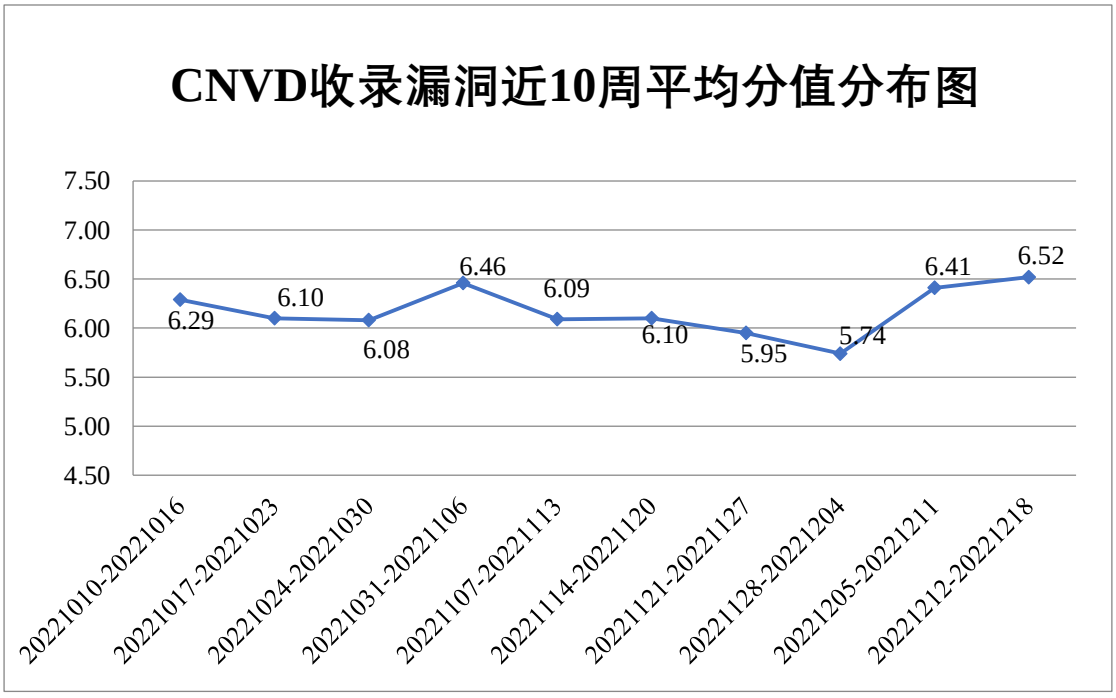

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 17 起，向基础电

信企业通报漏洞事件 55 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 674 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 96 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 81 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：

珠海新华通软件股份有限公司、众勤通信设备贸易（上海）有限公司、中软国际教育科技集团、中科美络科技股份有限公司、郑州众智科技股份有限公司、浙江中易慧能科技有限公司、浙江中控技术股份有限公司、浙江海看科技集团有限公司、浙江艾罗电源有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、五株科技股份有限公司、苏州华兆科技有限公司、视联动力信息技术股份有限公司、深圳市四海众联网络科技有限公司、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、深圳神州讯盟软件有限公司、上海银宇信息技术有限公司、上海商派网络科技有限公司、上海锐道信息技术有限公司、上海穆云智能科技有限公司、上海寰创通信科技股份有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海爱数信息技术股份有限公司、商丘芝麻开门网络科技有限公司、山东中创软件商用中间件股份有限公司、山东欧倍尔软件科技有限责任公司、全讯汇聚网络科技（北京）有限公司、青岛易软天创网络科技有限公司、南京涌亿思信息技术有限公司、南京汇龙科技有限公司、南方数据、理光（中国）投资有限公司、劲旅环境科技股份有限公司、江苏省广电有线信息网络股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、弘扬软件股份有限公司、广州市动景计算机科技有限公司、高通企业管理（上海）有限公司、福建星网锐捷通讯股份有限公司、帆软软件有限公司、帝兴软件开发有限公司、大连华天软件有限公司、成都零起飞科技有限公司、北京智邦国际软件技术有限公司、北京一采通信息科技有限公司、北京星网锐捷网络技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京天融信科技有限公司、北京宏景世纪软件股份有限公司、北京大为知创科技有限公司、北京博搜网络信息技术有限公司、阿里巴巴集团安全应急响应中心、Teledyne FLIR 和 NETGEAR。

本周，CNVD 发布了《Microsoft 发布 2022 年 12 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8386

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、新华三技术有限公司、

安天科技集团股份有限公司、西安四叶草信息技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。中国电信股份有限公司网络安全产品运营中心、北京华顺信安信息技术有限公司、西门子（中国）有限公司、北京山石网科信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州默安科技有限公司、赛尔网络有限公司、河南东方云盾信息技术有限公司、博智安全科技股份有限公司、安徽锋刃信息科技有限公司、重庆易阅科技有限公司、重庆都会信息科技有限公司、山东九域信息技术有限公司、苏州棱镜七彩信息科技有限公司、快页信息技术有限公司、浙江木链物联网科技有限公司、上海纽盾科技股份有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、江苏易安联网络技术有限公司、任子行网络技术股份有限公司、广州安亿信软件科技有限公司、联通数字科技有限公司、杭州美创科技有限公司、海南神州希望网络有限公司、中通服创发科技有限责任公司、山东云天安全技术有限公司、北京六方云信息技术有限公司、统信软件技术有限公司、河南悦海数安科技有限公司、广东唯顶信息科技股份有限公司、南方电网数字电网研究院有限公司、山石网科通信技术股份有限公司、北京冠程科技有限公司、云南联创网安科技有限公司、北京安帝科技有限公司、北京微步在线科技有限公司、河北千诚电子科技有限公司、联通沃悦读科技文化有限公司、中科国宏科技有限公司、浙江信安昆仑信息技术有限公司、北京瑾逸海阔科技有限公司、万宗网络科技（上海）有限公司、河南信安世纪科技有限公司、听潮盛世（北京）科技有限公司、贵阳朗迅岚科技有限公司、江西和尔惠信息技术有限公司、上海谋乐网络科技有限公司及其他个人白帽子向 CNVD 提交了 26350 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24825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）	22748	22748
斗象科技（漏洞盒子）	878	878
三六零数字安全科技集团有限公司	843	843
上海交大	356	356
深信服科技股份有限公司	314	0
新华三技术有限公司	299	0
安天科技集团股份有限公司	292	0

西安四叶草信息技术有限公司	205	205
北京启明星辰信息安全技术有限公司	162	0
北京神州绿盟科技有限公司	148	1
内蒙古云科数据服务股份有限公司	63	63
杭州安恒信息技术股份有限公司	52	25
恒安嘉新（北京）科技股份公司	30	0
中国电信集团系统集成有限责任公司	27	0
卫士通信息产业股份有限公司	22	22
杭州迪普科技股份有限公司	20	1
京东科技信息技术有限公司	13	0
浙江大华技术股份有限公司	3	3
北京天融信网络安全技术有限公司	3	3
北京信联科汇科技有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	237	0
北京华顺信安信息技术有限公司	208	3
西门子（中国）有限	54	0

公司		
北京山石网科信息技术有限公司	41	41
奇安星城网络安全运营服务（长沙）有限公司	28	28
杭州默安科技有限公司	26	26
赛尔网络有限公司	25	25
河南东方云盾信息技术有限公司	25	25
博智安全科技股份有限公司	22	22
安徽锋刃信息科技有限公司	20	20
重庆易阅科技有限公司	10	10
重庆都会信息科技有限公司	10	10
山东九域信息技术有限公司	9	9
苏州棱镜七彩信息科技有限公司	7	7
快页信息技术有限公司	6	6
浙江木链物联网科技有限公司	5	5
上海纽盾科技股份有限公司	5	5
山东新潮信息技术有限公司	4	4
河南灵创电子科技有限公司	3	3
江苏易安联网络技术有限公司	3	3

任子行网络技术股份有限公司	2	2
广州安亿信软件科技有限公司	2	2
联通数字科技有限公司	2	2
杭州美创科技有限公司	2	2
海南神州希望网络有限公司	2	2
中通服创发科技有限责任公司	2	2
山东云天安全技术有限公司	2	2
北京六方云信息技术有限公司	2	2
统信软件技术有限公司	2	2
河南悦海数安科技有限公司	2	2
广东唯顶信息科技股份有限公司	1	1
南方电网数字电网研究院有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京冠程科技有限公司	1	1
云南联创网安科技有限公司	1	1
北京安帝科技有限公司	1	1
北京微步在线科技有限公司	1	1
河北千诚电子科技有	1	1

限公司		
联通沃悦读科技文化有限公司	1	1
中科国宏科技有限公司	1	1
浙江信安昆仑信息技术有限公司	1	1
北京瑾逸海阔科技有限公司	1	1
万宗网络科技（上海）有限公司	1	1
河南信安世纪科技有限公司	1	1
听潮盛世（北京）科技有限公司	1	1
贵阳朗迅岚科技有限公司	1	1
江西和尔惠信息技术有限公司	1	1
上海谋乐网络科技有限公司	1	1
CNCERT 四川分中心	2	2
个人	908	908
报送总计	28176	26350

本周漏洞按类型和厂商统计

本周，CNVD 收录了 547 个漏洞。WEB 应用 245 个，应用程序 150 个，网络设备（交换机、路由器等网络端设备）84 个，智能设备（物联网终端设备）33 个，操作系统 19 个，数据库 9 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	245
应用程序	150
网络设备（交换机、路由器等网络端设备）	84

智能设备（物联网终端设备）	33
操作系统	19
数据库	9
安全产品	7

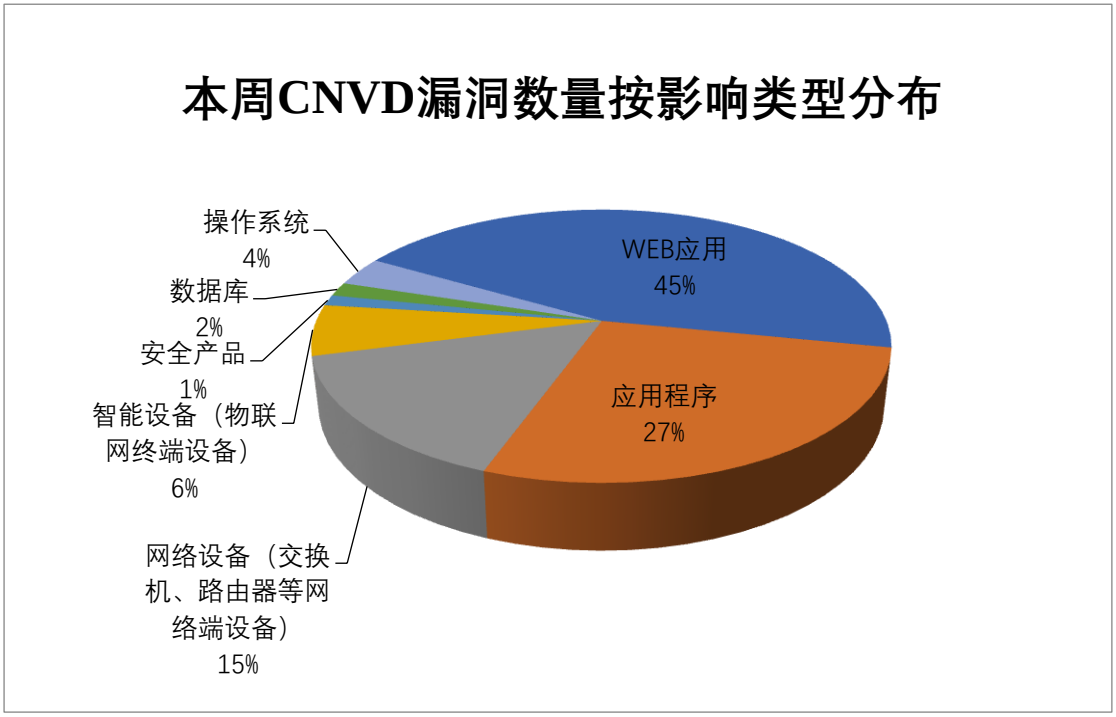

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Tenda、Siemens 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	WordPress	62	11%
2	Tenda	34	6%
3	Siemens	22	4%
4	MediaTek	15	3%
5	Huawei	14	3%
6	Adobe	14	3%
7	Samsung	12	2%
8	Cisco	11	2%
9	WordPress	11	2%
10	其他	352	64%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，32 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Apple iOS 拒绝服务漏洞、Siemens SCALANCE X-200RNA Switch Devices 不受控制资源消耗漏洞（CNVD-2022-87967）”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/

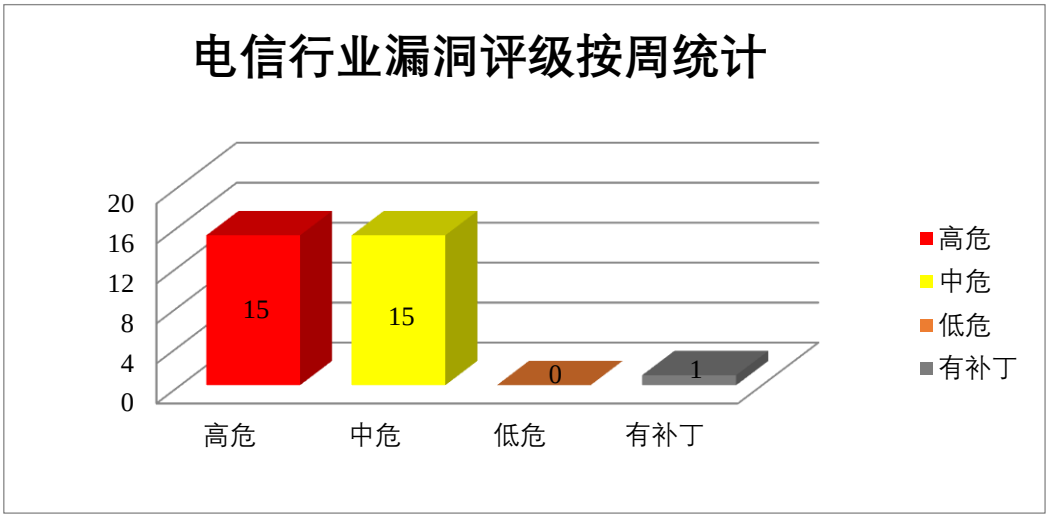

图 3 电信行业漏洞统计

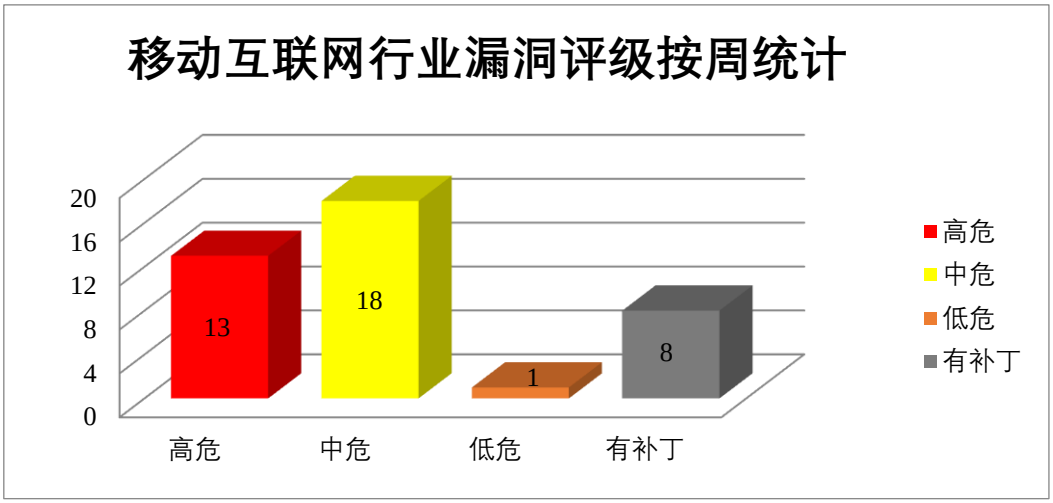

图 4 移动互联网行业漏洞统计

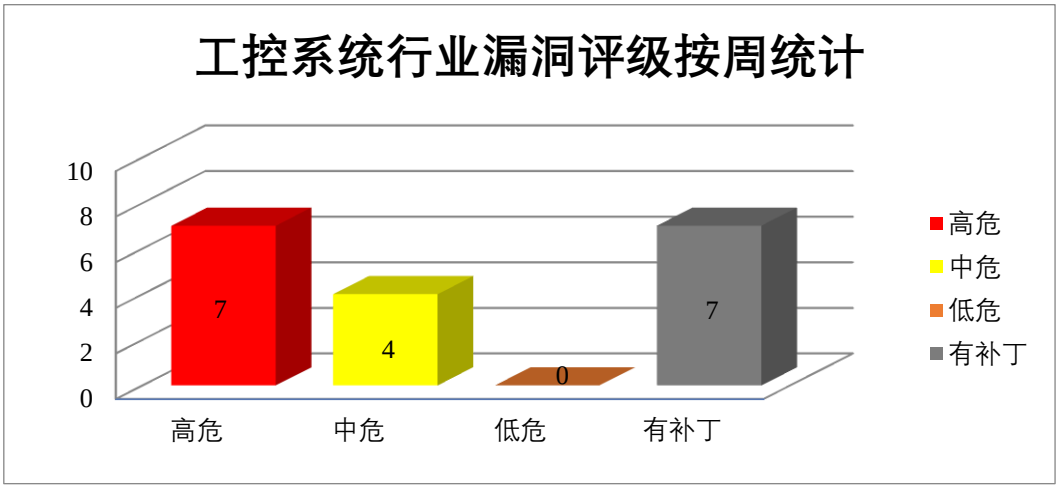

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens Parasolid 是德国西门子（Siemens）公司的一个几何建模内核。SIMATIC Drive Controllers 用于生产机器的自动化，结合了 SIMATIC S7-1500 CPU 和 SINAMIC S S120 驱动控制的功能。SIMATIC ET 200SP Open Controller 是 SIMATIC S7-1500 控制器的基于 PC 的版本。SIMATIC S7-1200 CPU 产品专为工业环境中的离散和连续控制而设计，如全球制造业、食品和饮料以及化工行业。SIMATIC S7-1500 CPU 产品专为全球制造、食品和饮料以及化工等工业环境中的离散和连续控制而设计。SIMATIC S7-1500 Software Controller 是用于基于 PC 的自动化解决方案的 SIMATIC 软件控制器。SIMATIC S7-PLCSIM Advanced 模拟 S7-1200、S7-1500 和其他一些 PLC 衍生产品。包括模拟 PLC 的完全网络访问，即使在虚拟化环境中也是如此。SIPLUS extreme 产品设计用于在极端条件下可靠运行，基于 SIMATIC，LOGO!，SITOP，SINAMICS，SIMOTION，SCALANCE 或其他设备。SIPLUS 设备使用与其所基于的产品相同的固件。TIM 1531 IRC 是 SIMATIC S7-1500、S7-400、S7-300 与 SINAUT ST7、DNP3 和 IEC 60870-5-101/104 的通信模块，具有三个 RJ45 接口，用于通过基于 IP 的网络（WAN/LAN）进行通信，以及一个 RS 232/RS 485 接口，用于经经典 WAN 网络进行通信。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在设备中拒绝服务，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（CNVD-2022-87977、CNVD-2022-87979、CNVD-2022-87978、CNVD-2022-87980）、Siemens Industrial 产品拒绝服务漏洞（CNVD-2022-87982、CNVD-2022-87984、CNVD-2022-87983、CNVD-2022-87985）。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-2022-87977

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87979

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87978

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87980

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87982

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87984

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87983

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87985

2、Oracle 产品安全漏洞

Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。Java VM 是其中的一个 Java 虚拟机组件。Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Oracle MySQL Server 是一款关系型数据库。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过 HTTP 访问网络，从而破坏 Oracle Enterprise Data Quality，对 Oracle Enterprise Data Quality 的关键数据和所有可访问数据，导致对 Java VM 可访问数据的子集进行未经授权的读取访问，通过多种协议访问网络，从而破坏 MySQL Server，并导致 MySQL Server 挂起或频繁重复崩溃（完全 DOS）等。

CNVD 收录的相关漏洞包括：Oracle Database Server 信息泄露漏洞（CNVD-2022-87654）、Oracle Enterprise Data Quality 信息泄露漏洞、Oracle MySQL Server 拒绝服务漏洞（CNVD-2022-87656、CNVD-2022-87655、CNVD-2022-87659、CNVD-2022-87658、CNVD-2022-87657、CNVD-2022-87660）。其中，“Oracle Enterprise Data Quality 信息泄露漏洞”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-2022-87654

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87653

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87656

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87655

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87659

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87658

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87657

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87660

3、IBM 产品安全漏洞

IBM WebSphere MQ 是美国国际商业机器（IBM）公司的一套系统。IBM Sterling

Secure Proxy 是一个用于确保组织非保护区(DMZ)中文件安全传输的应用程序代理。IBM PowerVM Hypervisor 是一个应用软件。提供了一个安全且可扩展的虚拟化环境，这些应用程序基于 Power Systems 平台的高级 RAS 功能和领先性能而构建。IBM Sterling Partner Engagement Manager 是一个自动化管理工具。IBM Security Access Manager Appliance（ISAM Appliance）是一款基于网络设备的安全解决方案。该产品主要用于访问控制和基于 Web 的威胁防护，提供系统性能监控、日志分析和诊断等功能。IBM Engineering Requirements Quality Assistant 是一款基于 Watson AI 用于辅助开发人员提高工程需求质量的软件。该应用可显著降低发现缺陷成本，有利于尽早发现工程流程中的需求错误，加快产品上市。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞解密高度敏感的信息，绕过安全配置设置并导致拒绝服务，获得提升的权限等。

CNVD 收录的相关漏洞包括：IBM WebSphere MQ 拒绝服务漏洞（CNVD-2022-87643）、IBM Sterling Secure Proxy 弱加密漏洞、IBM PowerVM Hypervisor 配置错误漏洞、IBM Sterling Partner Engagement Manager 跨站请求伪造漏洞、IBM Sterling Partner Engagement Manager 服务器端请求伪造漏洞、IBM Sterling Partner Engagement Manager LDAP 注入漏洞、IBM Security Access Manager Appliance 访问控制错误漏洞（CNVD-2022-87650）、IBM Engineering Requirements Quality Assistant 跨站脚本漏洞（CNVD-2022-87649）。其中，除“IBM Sterling Partner Engagement Manager 服务器端请求伪造漏洞、IBM Security Access Manager Appliance 访问控制错误漏洞（CNVD-2022-87650）、IBM Engineering Requirements Quality Assistant 跨站脚本漏洞（CNVD-2022-87649）”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-2022-87643

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87642

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87644

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87648

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87647

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87646

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87650

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87649

4、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。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。Adobe Framemaker 是一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Dimension 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

漏洞在系统上执行代码或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-87164、CNVD-2022-87165）、多款 Adobe 产品资源管理错误漏洞、Adobe Frame Maker 堆缓冲区溢出漏洞（CNVD-2022-87169、CNVD-2022-87168）、Adobe Dimension 内存错误引用漏洞、Adobe Dimension 代码执行漏洞、Adobe Dimension 越界读取漏洞。其中，除“Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-87164、CNVD-2022-87165）”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-2022-87164

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87165

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87166

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87168

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87169

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87921

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87920

https://www.cnvd.org.cn/flaw/show/CNVD-2022-87923

5、WordPress Read more By Adam 跨站请求伪造漏洞

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。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 plugin 是一个应用插件。本周，WordPress Read more By Adam 被披露存在跨站请求伪造漏洞。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。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-2022-88226

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-2022-87014	WordPress Plugin Betheme them plugin 反序列化漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.wordfence.com/vulnerability-advisories-continued/#CVE-2022-3861
CNVD-2022-87017	WordPress WP User Frontend 授权问题漏洞	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/9486744e-ab24-44e4-b06e-9e0b4be132e

			2
CNVD-2022-87039	Samsung FeedsInfo 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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6
CNVD-2022-87041	Samsung LSOItemData 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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6
CNVD-2022-87170	Fortinet FortiOS SSLVPN 远程代码执行漏洞	高	Fortinet 官方已发布新版本进行漏洞修复，受影响的用户可升级到如下安全版本进行漏洞修复：https://www.fortiguard.com/psirt/FG-IR-22-398
CNVD-2022-87255	Google TensorFlow BaseCandidateSamplerOp 缓冲区错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j
CNVD-2022-87257	Google TensorFlow tf.raw_ops.FusedResizeAndPadConv2D 缓冲区溢出漏洞	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/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx
CNVD-2022-87256	Google TensorFlow tf.keras.losses.poisson 缓冲区溢出漏洞	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/tensorflow/tensorflow/security/advisories/GHSA-8fvv-46hw-vpg3
CNVD-2022-87259	JetBrains Hub 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.jetbrains.com/privacy-security/issues-fixed
CNVD-2022-87258	Google TensorFlow tf.raw_ops.ImageProjectiveTransformV2 缓冲区溢出漏洞	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/tensorflow/tensorflow/security/advisories/GHSA-54pp-c6pp-7fpx

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞在设备中拒绝服务，在当前进程的上下文中执行代码。此外，Oracle、IBM、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致对 Java VM 可访问数据的子集进行未经授权的

读取访问，解密高度敏感的信息，绕过安全配置设置并导致拒绝服务，获得提升的权限，在系统上执行代码或导致应用程序崩溃等。另外，WordPress Read more By Adam 被披露存在跨站请求伪造漏洞。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。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、ZKTeco ZKBioSecurity SQL 注入漏洞

验证描述

ZKTeco ZKBioSecurity 是中国 ZKTeco 公司的一个基于 Web 的一体式平台。

ZKteco ZKBioSecurity V5000 4.1.3 版本存在 SQL 注入漏洞，该漏洞源于组件/baseOpLog.do 缺少对外部输入 SQL 语句的验证，攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://medium.com/stolabs/cve-2022-36635-a-sql-injection-in-zksecuritybio-to-rce-c5bde2962d47

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-87368

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. Samba 发布安全更新以修补多个安全漏洞

Samba 已发布软件更新以修复多个漏洞，如果成功利用这些漏洞，攻击者可能会控制受影响的系统。Samba 是适用于 Linux、Unix 和 macOS 操作系统的开源 Windows 互操作性套件，可提供文件服务器、打印和 Active Directory 服务。

参考链接：https://thehackernews.com/2022/12/samba-issues-security-updates-to-patch.html

2. VMware 修复了 ESXi 和 vRealize 安全漏洞

VMware 发布了安全更新，以解决影响 ESXi、Workstation、Fusion 和 Cloud Foundation 的严重漏洞，以及影响 vRealize Network Insight 的命令注入漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-esxi-and-vrealize-security-flaws/

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