国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 02 月 07 日-2022 年 02 月 13 日 **2022 年第 6 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 528 个，其中高危漏洞 118 个、中危漏洞 371 个、低危漏洞 39 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 300 个（占 57%），其中互联网上出现“ZOHO ManageEngine Key Manager Plus 跨站脚本漏洞、Joomla! DT Register 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 2382 个，与上周（6178 个）环比减少 61%。

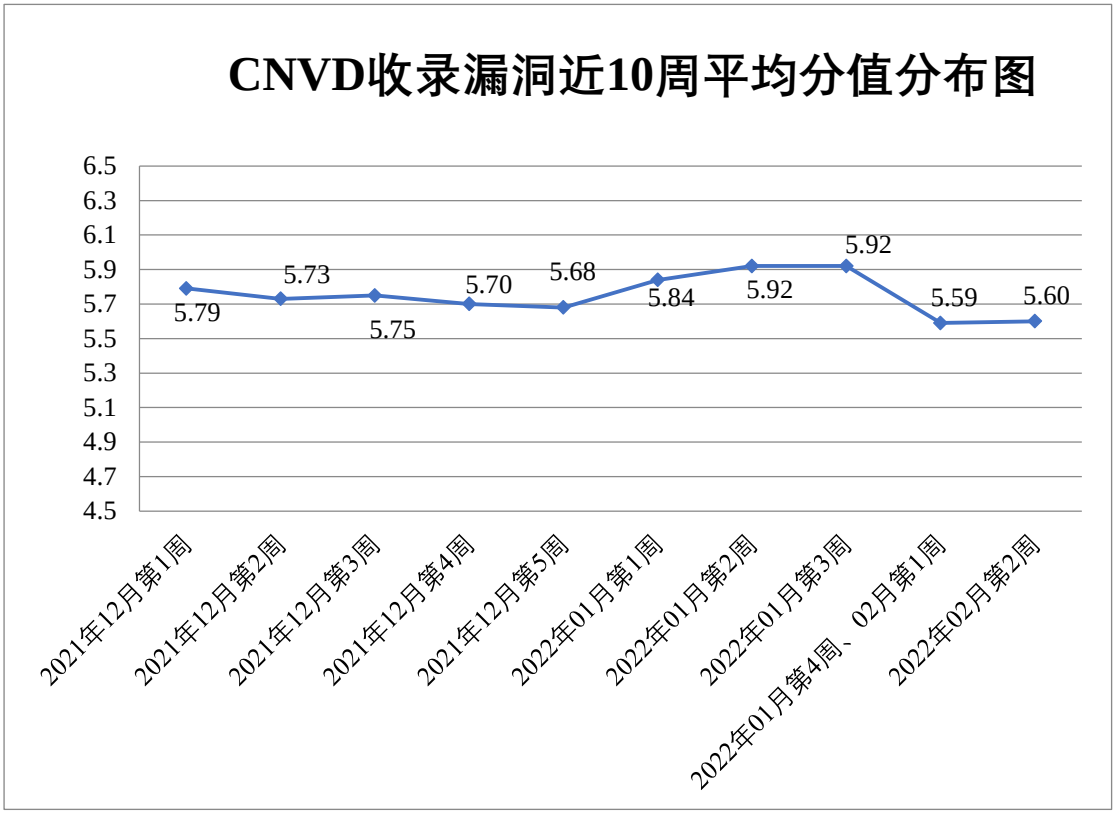

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 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 452 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 123 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 64 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：

法国施耐德电气（Schneider Electric）公司、广州商淘信息科技有限公司、思科系统（中国）网络技术有限公司、山东中创软件商用中间件股份有限公司、上海顶想信息科技有限公司、南宁旭东网络科技有限公司、大唐电信科技股份公司、广州添富信息科技有限公司、福建四创软件有限公司、西门子（中国）有限公司、四创科技有限公司、优酷信息技术（北京）有限公司、上海卓卓网络科技有限公司、武汉达梦数据库股份有限公司、北京莱桥通信技术有限公司、若依、深圳警翼智能科技股份有限公司、深圳市忆志科技有限公司、西安甜派网络科技有限公司、钉钉（中国）信息技术有限公司、安科瑞电气股份有限公司、北京通达志成科技有限公司、普联技术有限公司、兄弟（中国）商业有限公司、北京金和网络股份有限公司、北京爱奇艺科技有限公司、江西铭软科技有限公司、上海万欣计算机信息科技有限公司、上海赛连信息科技有限公司、柯尼卡美能达集团、合肥海拔网络科技有限公司、深圳市吉祥腾达科技有限公司、北京百度网讯科技有限公司、北京星网锐捷网络技术有限公司、BlueCMS、ebuycms、NETGEAR、LzCMS、Axis Communications AB、ZZCMS、emlog、yzmcms、FineCMS、CSCMS、The Apache Software Foundation、jpress、Cesanta。

本周，CNVD 发布了《Microsoft 发布 2022 年 2 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7366

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、北京天融信网络安全技术有限公司、安天科技集团股份有限公司、阿里云计算有限公司、杭州安恒信息技术股份有限公司等单位报送公开收集的漏洞数量较多。南京树安信息技术有限公司、山东云天安全技术有限公司、西门子（中国）有限公司、河南灵创电子科技有限公司、广东蓝爵网络安全技术股份有限公司、星云博创科技有限公司、北京网御星云信息技术有限公司、杭州默安科技有限公司、福建省海峡信息技术有限公司、北京华云安信息技术有限公司、

河南金盾信安检测评估中心、上海纽盾科技股份有限公司、河南信安世纪科技有限公司、山东新潮信息技术有限公司、墨菲安全、平安银河实验室、泰山信息科技有限公司、智网安云（武汉）信息技术有限公司、广西等保安全测评有限公司、上海上讯信息技术股份有限公司、博智安全科技股份有限公司、山石网科通信技术股份有限公司、思而听网络科技有限公司、北京山石网科信息技术有限公司、天津启明星辰信息技术有限公司及其他个人白帽子向 CNVD 提交了 2382 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 1099 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）	657	657
上海交大	336	336
斗象科技（漏洞盒子）	106	106
新华三技术有限公司	308	0
北京天融信网络安全技术有限公司	180	28
安天科技集团股份有限公司	166	0
阿里云计算有限公司	149	1
杭州安恒信息技术股份有限公司	147	56
厦门服云信息科技有限公司	139	0
北京神州绿盟科技有限公司	116	8
北京启明星辰信息安全技术有限公司	105	4
恒安嘉新（北京）科技股份公司	94	0
天津市国瑞数码安全系统股份有限公司	89	0
北京数字观星科技有限公司	51	0

远江盛邦（北京）网络安全科技股份有限公司	42	42
西安四叶草信息技术有限公司	31	31
中国电信集团系统集成有限责任公司	27	0
南京联成科技发展股份有限公司	8	8
内蒙古云科数据服务股份有限公司	8	8
南京众智维信息科技有限公司	2	2
北京知道创宇信息技术股份有限公司	1	0
南京树安信息技术有限公司	38	38
山东云天安全技术有限公司	27	27
西门子（中国）有限公司	24	0
河南灵创电子科技有限公司	20	20
广东蓝爵网络安全技术股份有限公司	17	17
星云博创科技有限公司	13	13
北京网御星云信息技术有限公司	10	10
杭州默安科技有限公司	7	7
亚信科技（成都）有限公司	7	0
福建省海峡信息技术	6	6

有限公司		
北京华云安信息技术有限公司	6	6
河南金盾信安检测评估中心	5	5
上海纽盾科技股份有限公司	5	5
河南信安世纪科技有限公司	3	3
山东新潮信息技术有限公司	2	2
墨菲安全	2	2
平安银河实验室	2	2
泰山信息科技有限公司	1	1
智网安云（武汉）信息技术有限公司	1	1
广西等保安全测评有限公司	1	1
上海上讯信息技术股份有限公司	1	1
博智安全科技股份有限公司	1	1
山石网科通信技术股份有限公司	1	1
思而听网络科技有限公司	1	1
北京山石网科信息技术有限公司	1	1
天津启明星辰信息技术有限公司	1	1
CNCERT 贵州分中心	7	7
CNCERT 内蒙古分中心	2	2

个人	914	914
报送合计	3888	2382

本周漏洞按类型和厂商统计

本周，CNVD 收录了 528 个漏洞。应用程序 249 个，WEB 应用 171 个，网络设备（交换机、路由器等网络端设备）45 个，数据库 24 个，智能设备（物联网终端设备）18 个，操作系统 14 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
应用程序	249
WEB 应用	171
网络设备（交换机、路由器等网络端设备）	45
数据库	24
智能设备（物联网终端设备）	18
操作系统	14
安全产品	7

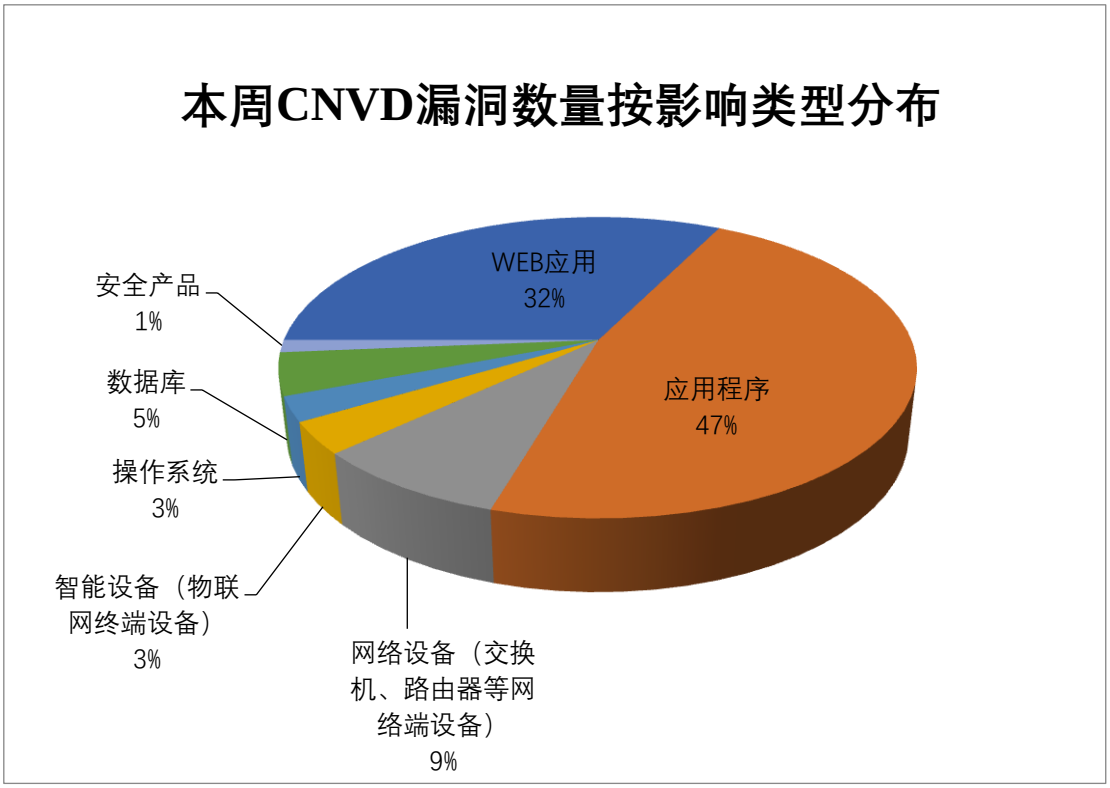

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cesanta、Oracle 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	Google	48	9%
2	Cesanta	24	5%
3	Oracle	21	4%
4	JetBrains	20	4%
5	SourceCodester	18	3%
6	Jerry	14	3%
7	深圳市吉祥腾达科技有限公司	13	2%
8	ZOHO	12	2%
9	Adobe	11	2%
10	其他	347	66%

本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，5 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，“Moxa TN-5900 命令注入漏洞、Zyxel GS1900 操作系统命令注入漏洞”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/

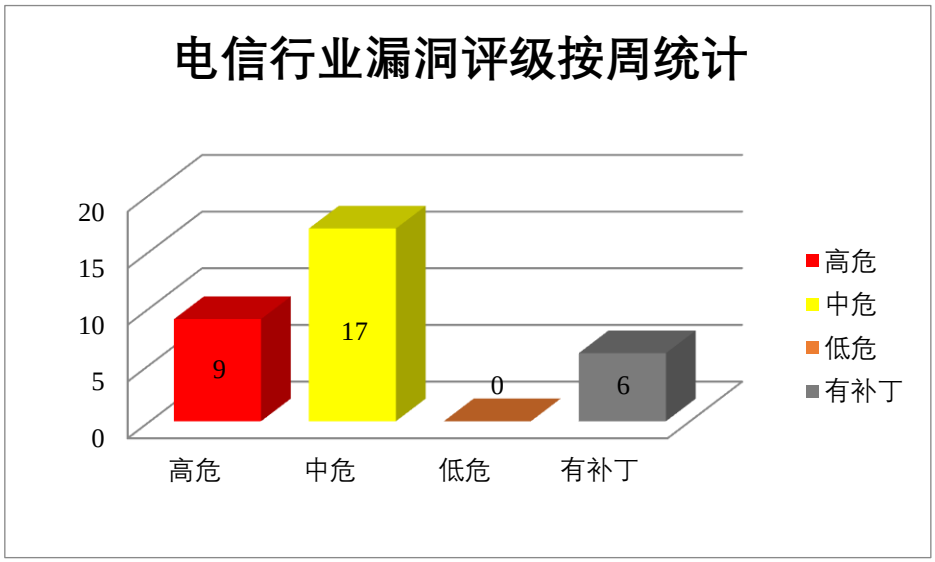

图 3 电信行业漏洞统计

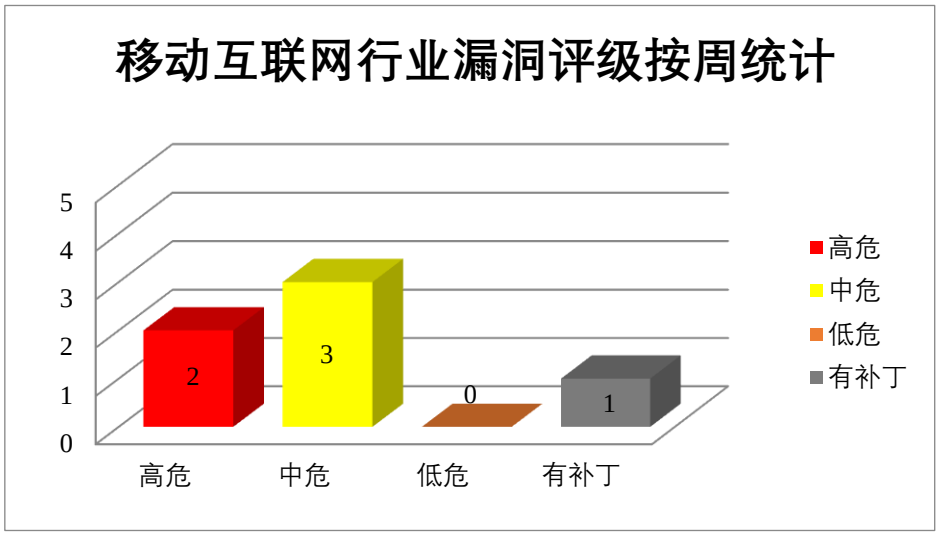

图 4 移动互联网行业漏洞统计

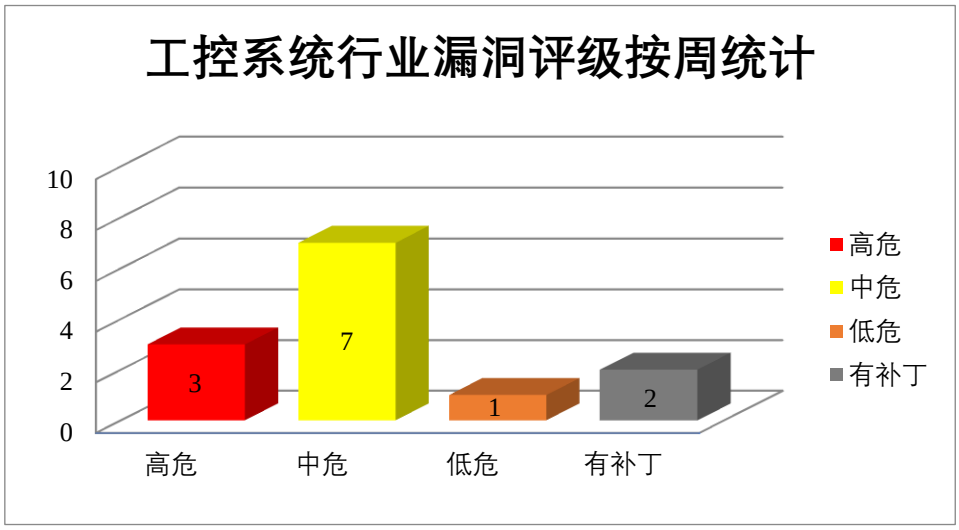

图 5 工控系统行业漏洞统计

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、 Oracle 产品安全漏洞

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞破坏或删除数据。

CNVD 收录的相关漏洞包括：Oracle MySQL 缓冲区溢出漏洞、Oracle MySQL 输入验证错误漏洞（CNVD-2022-09136、CNVD-2022-09135、CNVD-2022-09134、CNVD-2022-09139、CNVD-2022-09143、CNVD-2022-09142、CNVD-2022-09141）。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-2022-09133

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09136

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09135

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09134

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09139

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09143

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09142

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09141

2、 Apache 产品安全漏洞

Apache OpenOffice 是美国阿帕奇（Apache）基金会的一款开源的办公软件套件。该套件包含文本文档、电子表格、演示文稿、绘图、数据库等。Apache HTTP Server 是美国阿帕奇（Apache）软件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 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 Dubbo 是美国阿帕奇（Apache）基金会的一款基于 Java 的轻量级 RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。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。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发送特制的 XML 文件读取文件，在系统上提升权限，通过发送特制的 HTTP 请求造成拒绝服务（空指针逆向引用和段错误）等。

CNVD 收录的相关漏洞包括：Apache OpenOffice 访问控制错误漏洞、Apache HTTP Server mod_md 拒绝服务漏洞、Apache OpenOffic 内存破坏漏洞、Apache OpenOffice XML 外部实体注入漏洞、Apache HTTP Server 拒绝服务漏洞（CNVD-2022-09237）、Apache Airflow 跨站脚本漏洞（CNVD-2022-09242）、Apache Dubbo 代码问题漏洞、Apache Jena XML 外部实体注入漏洞。其中“Apache Dubbo 代码问题漏洞”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-2022-09236

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09234

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09239

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09238

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09237

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09242

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09241

https://www.cnvd.org.cn/flaw/show/CNVD-2022-09240

3、 IBM 产品安全漏洞

IBM Financial Transaction Manager 是美国 IBM 公司的一款金融事务管理器。该产品主要用于监控、跟踪和报告金融支付和交易。IBM Security Verify Access（ISAM）是美国 IBM 公司的一款提高用户访问安全的服务。IBM Security Guardium Insights 是美国 IBM 公司的一套数据安全解决方案。该产品支持数据分析、威胁警报、数据安全性审计和本地数据监控等功能。IBM Guardium Data Encryption（GDE）是美国 IBM 公司的一个应用软件。提供一个数据安全和合规性解决方案。IBM DB2 是美国 IBM 公司的一套关系型数据库管理系统。IBM Spectrum Copy Data Management 是美国国际商业机器公司（IBM）的实现数据中心副本管理流程的现代化、简化和自动化。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恶意和未经授权的行为，以系统上的任何用户身份进行身份验证，窃取经过身份验证的会话，可导致用户名枚举等。

CNVD 收录的相关漏洞包括：IBM Financial Transaction Manager 跨站请求伪造漏洞（CNVD-2022-08964）、IBM Security Verify Access 未授权访问漏洞、IBM Financial Transaction Manager 授权问题漏洞（CNVD-2022-08965）、IBM Security Guardium Insights 信息泄露漏洞（CNVD-2022-08968）、IBM Guardium Data Encryption 信息泄露漏洞（CNVD-2022-08967）、IBM Security Guardium Insights 输入验证错误漏洞、IBM Db2 信息泄露漏洞（CNVD-2022-08971）、IBM Spectrum Copy Data Management 未授权访问漏洞。其中“IBM Spectrum Copy Data Management 未授权访问漏洞”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-2022-08964
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08966
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08965
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08968
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08967
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08969
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08971
https://www.cnvd.org.cn/flaw/show/CNVD-2022-08970

4、ZOHO 产品安全漏洞

Zoho Corporation ManageEngine OpManager 是美国 Zoho Corporation 公司的一款综合性网络监控软件。用于管理路由器、防火墙、服务器、交换机和打印机。ZOHO ManageEngine Remote Access Plus 是美国卓豪（ZOHO）公司的一套远程访问解决方案。ZOHO ManageEngine ADManager Plus 是美国卓豪（ZOHO）公司的一套为使用 Windows 域的企业用户设计的微软活动目录管理软件。该软件能够协助 AD 管理员和帮助台技术人员进行日常管理工作，例如批量管理用户帐户和 AD 对象、给帮助台技术员指派基于角色的访问权限等。ZOHO ManageEngine EventLog Analyzer 是美国卓豪（ZOHO）

公司的一套系统、事件日志分析软件。该软件能够对全网范围内的主机、服务器、网络设备以及各种应用服务系统等产生的日志，进行全面收集和细致分析。ZOHO Manage Engine AssetExplorer 是美国卓豪（ZOHO）公司的一套资产管理软件。该软件提供资产跟踪、IT 资产的扫描和资产所有权的跟踪等功能。ZOHO ManageEngine ServiceDesk Plus（SDP）是美国卓豪（ZOHO）公司的一套基于 ITIL 架构的 IT 服务管理软件。该软件集成了事件管理、问题管理、资产管理 IT 项目管理、采购与合同管理等功能模块。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞访问审计目录，提交特殊的请求，可未授权访问系统，导致远程代码执行等。

CNVD 收录的相关漏洞包括：Zoho Corporation ManageEngine OpManager 授权问题漏洞、Zoho ManageEngine Remote Access Plus 信任管理问题漏洞（CNVD-2022-09267、CNVD-2022-09266）、Zoho ManageEngine ADManager Plus 代码问题漏洞、Zoho ManageEngine ADManager Plus 路径遍历漏洞、Zoho ManageEngine Eventlog Analyzer 路径遍历漏洞、ZOHO ManageEngine AssetExplorer 信任管理问题漏洞、ZOHO ManageEngine ServiceDesk Plus 授权问题漏洞。除“Zoho ManageEngine Remote Access Plus 信任管理问题漏洞（CNVD-2022-09267、CNVD-2022-09266）、Zoho ManageEngine ADManager Plus 路径遍历漏洞”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-2022-09263
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09267
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09266
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09265
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09264
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09270
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09269
https://www.cnvd.org.cn/flaw/show/CNVD-2022-09268

5、jeecg 访问控制错误漏洞

jeecg 是一个应用软件。一款基于代码生成器的智能开发平台。本周 jeecg 被披露存在访问控制错误漏洞。攻击者可利用该漏洞通过修改 lcoalPath 来访问敏感文件。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-2022-08923

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-2022-08453	Huawei HarmonyOS 缓冲区溢出漏洞（CNVD-2022-08453）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202111-0000001217889667
CNVD-2022-08726	CodeIgniter 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/codeigniter4/CodeIgniter4/commit/ce95ed5765256e2f09f3513e7d42790e0d6948f5
CNVD-2022-08724	McAfee Agent 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://kc.mcafee.com/corporate/index?page=content&id=SB10378
CNVD-2022-08733	Nagios XI 路径遍历漏洞（CNVD-2022-08733）	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://www.nagios.com/products/nagios-xi/
CNVD-2022-08919	Spinnaker 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://github.com/spinnaker/spinnaker/security/advisories/GHSA-9h7c-rfrp-gvgp
CNVD-2022-08918	McAfee TechCheck 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://service.mcafee.com/?articleId=TS103243
CNVD-2022-08922	AuthGuard 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://github.com/AuthGuard/AuthGuard
CNVD-2022-09129	SuiteCRM 信息泄露漏洞（CNVD-2022-09129）	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://docs.suitecrm.com/
CNVD-2022-09132	livehelperchat 跨站脚本漏洞（CNVD-2022-09132）	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/livehelperchat/livehelperchat/commit/d3b107aaa8ec10816acc762d60e7321079c21706
CNVD-2022-09244	Fortinet FortiWeb 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/advisory/FG-IR-21-166

小结：本周，Oracle 产品被披露存在多个漏洞，攻击者可利用该漏洞导致缓冲区溢出，整数溢出，提升权限等。此外，Apache、IBM、ZOHO 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞破坏或删除数据，访问审计目录，提交特殊的请求，可未授权访问系统，导致远程代码执行。另外，jeecg 被披露存在访问控制错误漏洞。攻击者可利用该漏洞通过修改 lcoalPath 来访问敏感文件。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、ZOHO ManageEngine Key Manager Plus 跨站脚本漏洞

验证描述

ZOHO ManageEngine Key Manager Plus 是卓豪（ZOHO）公司的一套基于 WEB 的 SSH 秘钥管理解决方案，它可以帮助您加固、控制、管理、监控及审计 SSH 秘钥，跨越秘钥的整个生命周期。它为管理员提供了可视化的 SSH 管理能力，帮助管理员有效控制秘钥文件的合理使用以及秘钥文件的合规性。

Zoho ManageEngine Key Manager Plus 6001 之前版本存在跨站脚本漏洞，攻击者可利用该漏洞在用户管理页面上存储 XSS，同时从 AD 导入恶意用户详细信息。

验证信息

POC 链接：https://raxis.com/blog/cve-2021-28382

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-09271

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. 500 家电商网站被植入信用卡窃取程序

安全公司 Sansec 报告有大约 500 家电商网站被黑客植入了信用卡窃取程序，在访客试图在网站上购买商品时窃取敏感的支付信息。

参考链接：https://www.solidot.org/story?sid=70633

2. CISA 命令美国联邦机构在 2 月 25 日之前更新 iPhone、Mac

美国网络安全和基础设施安全局 (CISA) 在其在野外利用的漏洞目录中添加了一个新漏洞，这是一个用于针对 iPhone、iPad 和 Mac 的 Apple WebKit 远程代码执行漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-update-iphones-macs-until-feb-25th/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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