国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 02 月 20 日-2023 年 02 月 26 日 **2023 年第 8 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 345 个，其中高危漏洞 202 个、中危漏洞 120 个、低危漏洞 23 个。漏洞平均分值为 6.64。本周收录的漏洞中，涉及 0day 漏洞 293 个（占 85%），其中互联网上出现“PbootCMS SQL 注入漏洞（CNVD-2023-11247）、SEMCMS Ant_Pro.php 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漏洞总数 10131 个，与上周（7975 个）环比增加 27%。

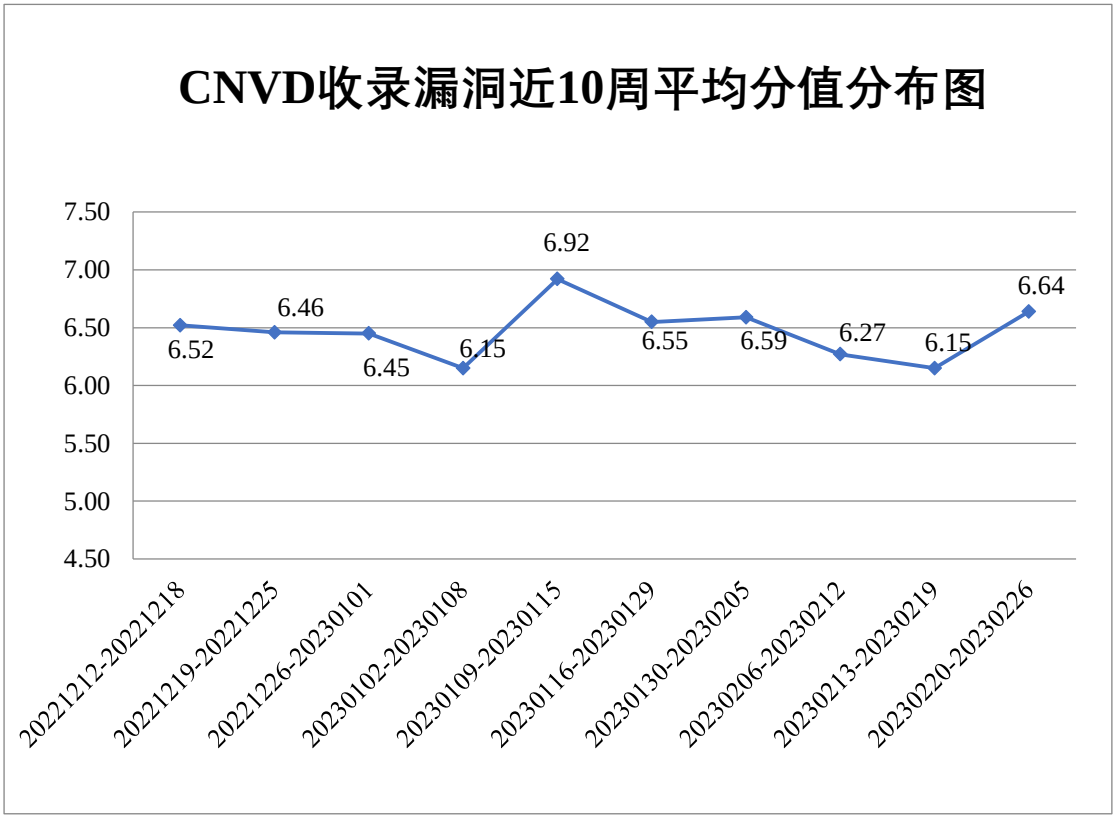

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 43 起，向基础电信企业通报漏洞事件 77 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 1211 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 109 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：

珠海迈科智能科技股份有限公司、浙江中控技术股份有限公司、友讯电子设备（上海）有限公司、武汉达梦数据库股份有限公司、通联支付网络服务股份有限公司、思迅软件（天津）有限责任公司、深圳智慧光迅信息技术有限公司、深圳市金信云服信息科技有限公司、深圳市和为顺网络技术有限公司、深圳市必联电子有限公司、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、上海博达数据通信有限公司、厦门天锐科技股份有限公司、麒麟软件有限公司、敬业钢铁有限公司、江苏叁拾叁信息技术有限公司、吉翁电子（深圳）有限公司、广东乾星信息科技股份有限公司、东莞市东城乔伦软件开发工作室、畅捷通信息技术股份有限公司、北京中农信达信息技术有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司和阿里巴巴集团安全应急响应中心。

本周，CNVD 发布了《关于 Joomla 存在未授权访问漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8601

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、北京启明星辰信息安全技术有限公司、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。北京升鑫网络科技有限公司、北京山石网科信息技术有限公司、上海齐同信息科技有限公司、快页信息技术有限公司、河南灵创电子科技有限公司、河南东方云盾信息技术有限公司、上海纽盾科技股份有限公司、内蒙古洞明科技有限公司、博智安全科技股份有限公司、安徽锋刃信息科技有限公司、湖南轻山信息技术有限公司、宁夏凯信特信息科技有限公司、山东鼎夏智能科技有限公司、内蒙古信元网络安全技术股份有限公司、河南省鼎信信息安全等级测评有限公司、江苏金盾检测技术有限公司、北京云梦创网络科技有限公司、内蒙古中叶信息技术有限责任公司、北京珞安科技有限责任公司、上海谋乐网络科技有限公司、赛尔网络有

限公司、北京微步在线科技有限公司、苏州棱镜七彩信息科技有限公司、北京东方通科技股份有限公司、福州启云信息技术有限公司、华泰证券股份有限公司、北京君云天下科技有限公司、山东云天安全技术有限公司及其他个人白帽子向 CNVD 提交了 10131 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）、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 7896 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）	3760	3760
斗象科技（漏洞盒子）	2015	2015
三六零数字安全科技集团有限公司	1288	1288
上海交大	833	833
深信服科技股份有限公司	721	0
新华三技术有限公司	355	0
安天科技集团股份有限公司	213	2
北京启明星辰信息安全技术有限公司	159	13
杭州安恒信息技术股份有限公司	154	154
北京神州绿盟科技有限公司	148	5
恒安嘉新（北京）科技股份公司	76	0
京东科技信息技术有限公司	15	1
南京众智维信息科技有限公司	10	10
中国电信集团系统集成有限责任公司	7	7
北京天融信网络安全技术有限公司	6	6

杭州迪普科技股份有限公司	2	2
北京知道创宇信息技术股份有限公司	2	0
西安四叶草信息技术有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
北京升鑫网络科技有限公司	89	89
北京山石网科信息技术有限公司	63	63
西门子（中国）有限公司	31	0
上海齐同信息科技有限公司	24	24
快页信息技术有限公司	20	20
河南灵创电子科技有限公司	14	14
河南东方云盾信息技术有限公司	12	12
上海纽盾科技股份有限公司	11	11
内蒙古洞明科技有限公司	9	9
博智安全科技股份有限公司	8	8
安徽锋刃信息科技有限公司	4	4
湖南轻山信息技术有限公司	4	4
宁夏凯信特信息科技有限公司	4	4

山东鼎夏智能科技有限公司	3	3
内蒙古信元网络安全技术股份有限公司	3	3
河南省鼎信信息安全等级测评有限公司	3	3
亚信科技（成都）有限公司	2	0
江苏金盾检测技术有限公司	2	2
北京云梦创网络科技有限公司	2	2
内蒙古中叶信息技术有限责任公司	2	2
北京珞安科技有限责任公司	2	2
上海谋乐网络科技有限公司	2	2
赛尔网络有限公司	1	1
北京微步在线科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
北京东方通科技股份有限公司	1	1
福州启云信息技术有限公司	1	1
华泰证券股份有限公司	1	1
北京君云天下科技有限公司	1	1
山东云天安全技术有限公司	1	1
CNCERT 贵州分中心	6	6
CNCERT 甘肃分中心	6	6

CNCERT 广西分中心	5	5
CNCERT 浙江分中心	4	4
个人	1723	1723
报送总计	11832	10131

本周漏洞按类型和厂商统计

本周，CNVD 收录了 345 个漏洞。WEB 应用 189 个，应用程序 114 个，网络设备（交换机、路由器等网络端设备）35 个，智能设备（物联网终端设备）5 个，操作系统 1 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
WEB 应用	189
应用程序	114
网络设备（交换机、路由器等网络端设备）	35
智能设备（物联网终端设备）	5
操作系统	1
安全产品	1

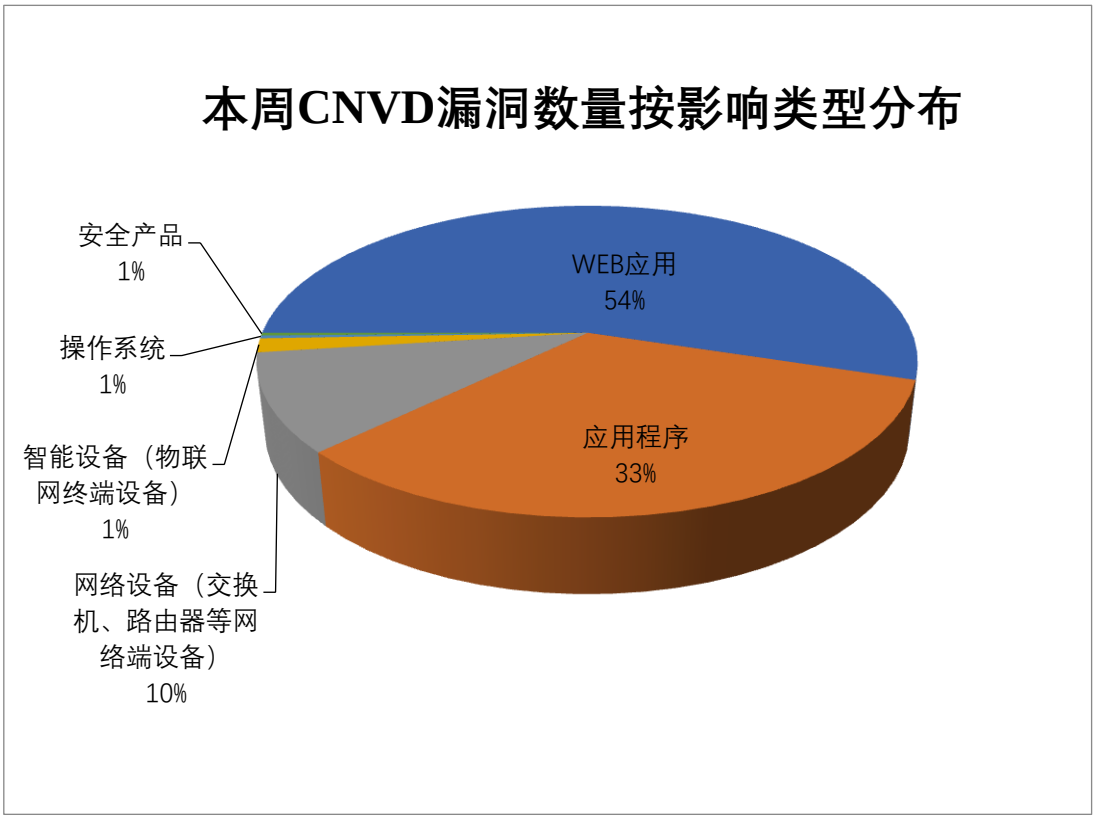

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 OTFCC、Carlo Montero、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	OTFCC	46	13%
2	Carlo Montero	27	7%
3	Google	11	3%
4	Pharmacy Management System	11	3%
5	SIEMENS	10	3%
6	商派软件有限公司	10	3%
7	D-Link	9	3%
8	IBM	9	3%
9	Oracle	9	3%
10	其他	203	59%

本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，16 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。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/

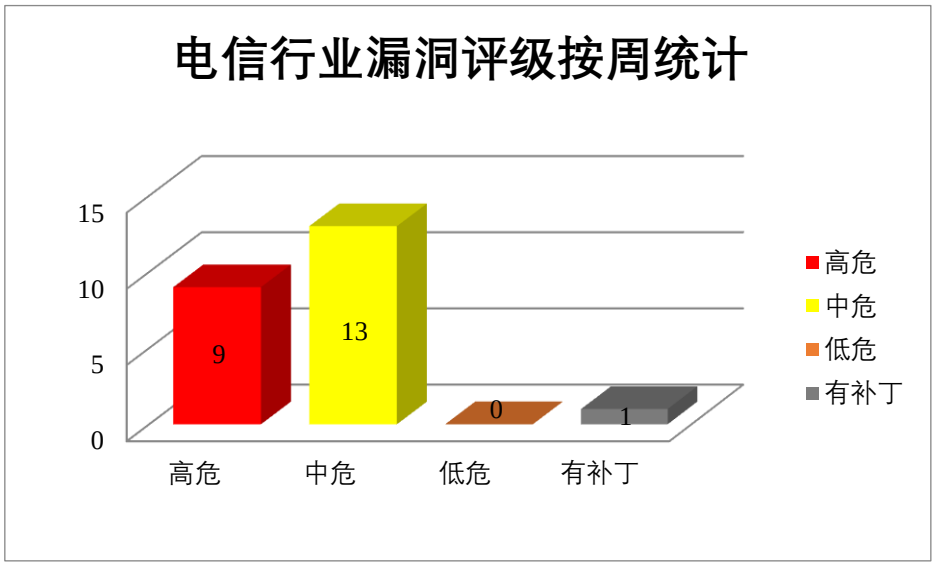

图 3 电信行业漏洞统计

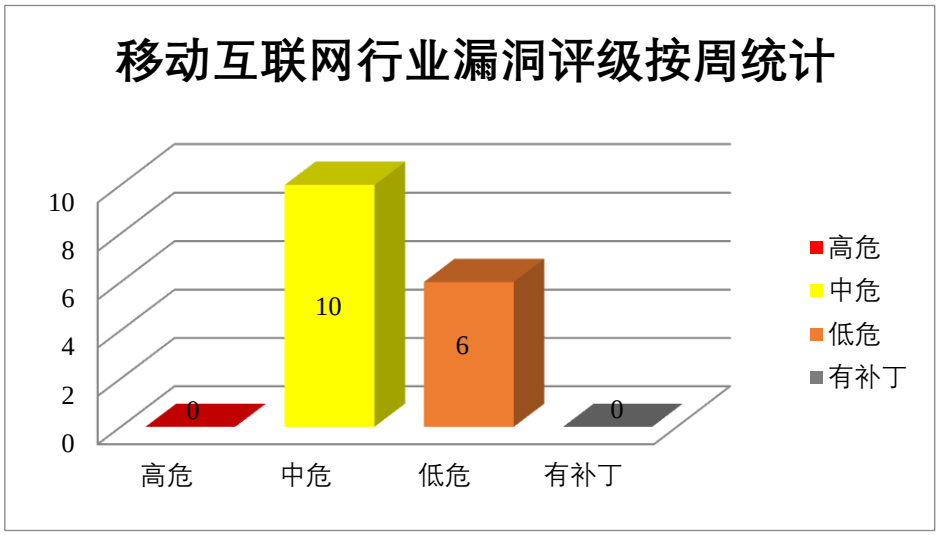

图 4 移动互联网行业漏洞统计

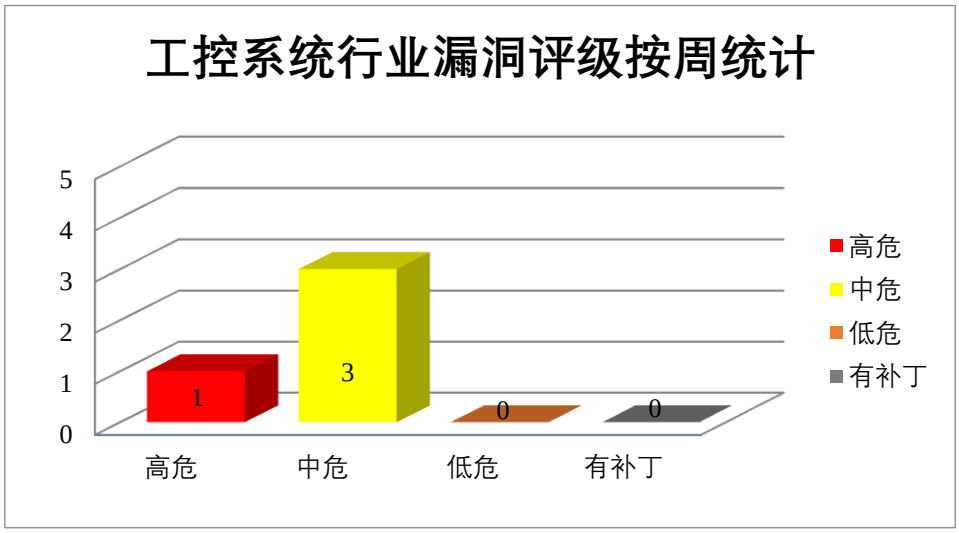

图 5 工控系统行业漏洞统计

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 TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞触发拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google TensorFlow 拒绝服务漏洞（CNVD-2023-10600、CNVD-2023-10601）、Google TensorFlow CollectiveGather 拒绝服务漏洞、Google TensorFlow 输入验证错误漏洞（CNVD-2023-10603）、Google TensorFlow AvgPoolOp 拒绝服务漏洞、Google TensorFlow EmptyTensorList 拒绝服务漏洞、Google TensorFlow DrawBoundingBoxes 拒绝服务漏洞、Google TensorFlow Conv2D 拒绝服务漏洞。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-2023-10600

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10604

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10603

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10602

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10601

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10607

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10606

https://www.cnvd.org.cn/flaw/show/CNVD-2023-10605

2、IBM 产品安全漏洞

IBM Maximo Asset Management 是美国国际商业机器（IBM）公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM Aspera 是美国国际商业机器（IBM）公司的一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM InfoSphere Information Server 是企业级信息集成平台。它能够帮助客户理解异构系统中的各种复杂信息，并且通过清洗和转换生成一致、完整的可信赖信息，最后将可信赖信息以各种方式交付给各种业务系统。IBM Sterling B2B Integrator 是美国国际商业机器（IBM）公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。IBM QRadar SIEM 是美国国际商业机器（IBM）公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。IBM WebSphere Application Server（WAS）是美国国际商业机器（IBM）公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在浏览器中返回详细的技术错误消息时获取敏感信息，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Maximo Asset Management 信息泄露漏洞（CNVD-2023-11691）、IBM Aspera Faspex 反序列化漏洞、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2023-11689）、IBM Aspera Faspex 跨站脚本漏洞、IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2023-11694）、IBM QRadar SIEM 信息泄露漏洞（CNVD-2023-11693）、IBM Sterling B2B Integrator 身份验证错误漏洞、IBM WebSphere Application Server 加密问题漏洞。其中，“IBM Aspera Faspex 反序列化漏洞”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-2023-11691

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11690

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11689

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11695

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11694

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11693

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11692

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11696

3、Oracle 产品安全漏洞

Oracle PeopleSoft Enterprise PeopleTools 是美国甲骨文（Oracle）公司的用于为 PeopleSoft 应用程序提供与用户的需求和期望保持同步的技术。Oracle Supply Chain Products Suite 是美国甲骨文（Oracle）公司的一套供应链解决方案。该产品提供价值链计划、价值链执行、产品生命周期管理等功能。Oracle PeopleSoft Enterprise PeopleTools 是美国甲骨文（Oracle）公司的用于为 PeopleSoft 应用程序提供与用户的需求和期望保持同步的技术。Oracle E-Business Suite（电子商务套件）是美国甲骨文（Oracle）公司的一套全面集成式的全球业务管理软件。该软件提供了客户关系管理、服务管理、财务管理等功能。Oracle VM VirtualBox 是美国甲骨文（Oracle）公司的一款虚拟机管理软件。Oracle Enterprise Manager Base Platform 是美国甲骨文（Oracle）公司的一套本地管理平台。该平台主要用于管理 Oracle 产品部署。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限制，在系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括 Oracle PeopleSoft Enterprise PeopleTools 信息泄露漏洞（CNVD-2023-11165、CNVD-2023-12017）、Oracle Supply Chain 信息泄露漏洞（CNVD-2023-11168）、Oracle PeopleSoft Enterprise PeopleTools 跨站脚本漏洞、Oracle Trade Management 信息泄露漏洞（CNVD-2023-11172）、Oracle VM VirtualBox 输入验证错误漏洞（CNVD-2023-11171）、Oracle Enterprise Manager Base Platform 输入验证错误漏洞、Oracle VM VirtualBox 拒绝服务漏洞（CNVD-2023-11169）。其中，“Oracle Enterprise Manager Base Platform 输入验证错误漏洞”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-2023-11165

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11168

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11166

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11172

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11171

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11170

https://www.cnvd.org.cn/flaw/show/CNVD-2023-11169

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12017

4、 Siemens 产品安全漏洞

Siemens Tecnomatix Plant Simulation 是面向对象的、图形化的、集成的建模、仿真工具。本周，上述产品被披露存在越界写入漏洞，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 Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-10614、CNVD-2023-10616、CNVD-2023-10615、CNVD-2023-10618、CNVD-2023-10617、CNVD-2023-10620、CNVD-2023-10619、CNVD-2023-10621）。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-2023-10614
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10616
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10615
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10618
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10617
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10620
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10619
https://www.cnvd.org.cn/flaw/show/CNVD-2023-10621

5、OTFCC 代码问题漏洞

OTFCC 是 Caryll 开源的一个 C 库和实用程序。用于解析和编写 OpenType 字体文件。本周，OTFCC 被披露存在代码问题漏洞。攻击者可利用该漏洞导致程序拒绝服务。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-2023-12000

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-2023-10610	Google TensorFlow 代码问题漏洞（CNVD-2023-10610）	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-828c-5j5q-vrjq
CNVD-2023-10609	Google TensorFlow 代码问题漏洞（CNVD-2023-10609）	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-qxpx-j395-pw36
CNVD-2023	Google TensorFlow 拒绝服务	高	目前厂商已发布升级补丁以修复漏

-10608	漏洞（CNVD-2023-10608）		洞，补丁获取链接：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9fpg-838v-wpv7
CNVD-2023-10611	Google TensorFlow 输入验证错误漏洞（CNVD-2023-10611）	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-v6h3-348g-6h5x
CNVD-2023-10613	Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-10613）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf
CNVD-2023-10612	Siemens JT Open Toolkit 堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf
CNVD-2023-11024	Joomla!未授权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新:https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html
CNVD-2023-11698	WordPress plugin 0mk Shortener 跨站请求伪造漏洞	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/threat-intel/vulnerabilities/id/3b798c64-3434-427d-b578-5abbdac8cd0e
CNVD-2023-11444	Simple E-Learning System search.php SQL 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://www.sourcecodester.com/php-simple-e-learning-system-source-code
CNVD-2023-11170	Oracle Enterprise Manager Base Platform 输入验证错误漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://www.oracle.com/security-alerts/cpujul2022.html

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞触发拒绝服务攻击。此外，IBM、Oracle、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在浏览器中返回详细的技术错误消息时获取敏感信息，在系统上执行任意代码等。另外，OTFCC 被披露存在代码问题漏洞。攻击者可利用该漏洞导致程序拒绝服务。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、PbootCMS SQL 注入漏洞（CNVD-2023-11247）

验证描述

PbootCMS 是 PbootCMS 个人开发者的一款使用 PHP 语言开发的开源企业建站内容管理系统（CMS）。

PbootCMS 3.0.5 版本存在安全漏洞。攻击者可利用该漏洞通过特制的 GET 请求执行任意 SQL 命令。

验证信息

POC 链接：https://github.com/penson233/Vuln/issues/3

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-11247

信息提供者

恒安嘉新（北京）科技股份公司

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. 数百个 Docker 容器镜像中隐藏漏洞，下载量高达数十亿次

Rezilion 发现了数百个 Docker 容器镜像的存在，这些镜像包含了大多数标准漏洞扫描器和 SCA 工具都没有检测到的漏洞。

参考链接：https://www.helpnetsecurity.com/2023/02/23/hidden-vulnerabilities-docker-containers/

2. 谷歌发布 Chrome 浏览器更新修复 10 个漏洞

谷歌 23 日面向 macOS、Linux 和 Windows 平台，发布了 Chrome 110.0.5481.177 .178 版本更新。本次更新主要修复了 10 个漏洞，其中包括 1 个“关键”级别的安全漏洞。

参考链接：http://www.anquan419.com/knews/24/4457.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