

信息安全漏洞周报

2023年02月13日-2023年02月19日

2023年第7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 351 个，其中高危漏洞 144 个、中危漏洞 174 个、低危漏洞 33 个。漏洞平均分为 6.15。本周收录的漏洞中，涉及 0day 漏洞 240 个（占 68%），其中互联网上出现“MonikaBrzica scm SQL 注入漏洞、Open5GS 拒绝服务漏洞（CNVD-2023-08774）”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 7975 个，与上周（5640 个）环比增加 41%。

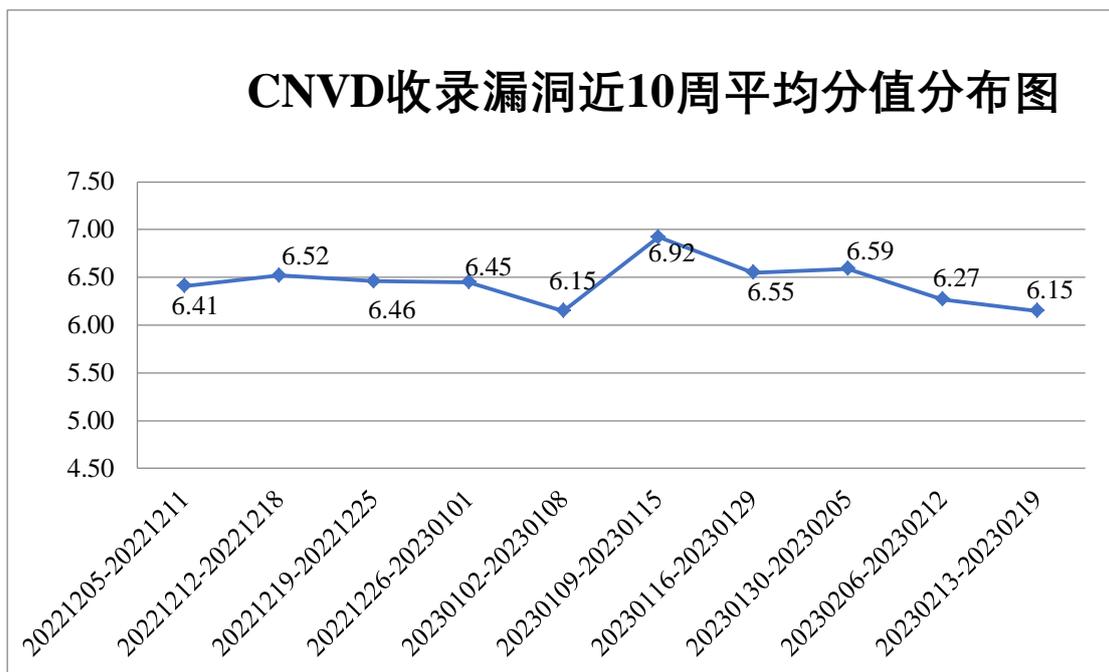


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 116 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 1084 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 151 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 118 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：

中兴通讯股份有限公司、中山市聚云软件科技有限公司、中山佳维电子有限公司、中科博华信息科技有限公司、浙江宇视科技有限公司、浙江永拓信息科技有限公司、浙江码尚科技股份有限公司、浙江宏伟供应链集团股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、熊猫智慧水务有限公司、武汉达梦数据库股份有限公司、武汉初心科技有限公司、神州数码控股有限公司、深圳维盟科技股份有限公司、深圳市智联物联科技有限公司、深圳市腾讯计算机系统有限公司、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、深圳市华脉智联科技有限公司、深圳市必联电子有限公司、上海英立视数字科技有限公司、上海我云网络科技有限公司、上海桑锐电子科技股份有限公司、上海泛微网络科技股份有限公司、熵基科技股份有限公司、商派软件有限公司、山东五征集团有限公司、山东开创集团股份有限公司、若依、青岛易软天创网络科技有限公司、千城智联（上海）网络科技有限公司、麒麟软件有限公司、品茗科技股份有限公司、鹏为软件股份有限公司、宁夏智林智能科技有限公司、迈普通信技术股份有限公司、浪潮通用软件有限公司、蓝盾信息安全技术有限公司、开封市文化旅游股份有限公司、吉翁电子（深圳）有限公司、华录智达科技股份有限公司、华录出版传媒有限公司、湖南建研信息技术股份有限公司、湖北京山轻工机械股份有限公司、杭州易由信息技术有限公司、杭州图特信息科技有限公司、杭州海康威视数字技术股份有限公司、福建银达汇智信息科技股份有限公司、东方网力科技股份有限公司、得力集团有限公司、成都智达万应科技有限公司、成都任我行软件股份有限公司、北京中园搏望科技发展有限公司、北京中成科信科技发展有限公司、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、北京统御至诚科技有限公司、北京神州视翰科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京火山引擎科技有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、安徽省科大奥锐科技有限公司、阿里巴巴集团安全应急响应中心和 OPPO 安全应急响应中心。

本周，CNVD 发布了《Microsoft 发布 2023 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/8576>

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、北京启明星辰信息安全技术有限公司、深信服科技股份有限公司、厦门服云信息科技有限公司、北京神州绿盟科技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、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、奇安星城网络安全运营服务(长沙)有限公司、西门子(中国)有限公司、上海齐同信息科技有限公司、北京山石网科信息技术有限公司、快页信息技术有限公司、杭州默安科技有限公司、安徽锋刃信息科技有限公司、内蒙古洞明科技有限公司、苏州棱镜七彩信息科技有限公司、山东新潮信息技术有限公司、云南联创网安科技有限公司、湖南轻山信息技术有限公司、河南灵创电子科技有限公司、星云博创科技有限公司、华泰证券股份有限公司、宁夏凯信特信息科技有限公司、江苏耘和计算机工程有限公司、上海谋乐网络科技有限公司、赛尔网络有限公司、北京华顺信安信息技术有限公司、任子行网络技术股份有限公司、墨菲未来科技(北京)有限公司、亚信科技(成都)有限公司、杭州美创科技有限公司、北京网御星云信息技术有限公司、武汉非尼克斯软件技术有限公司、北京快手科技有限公司、山东云天安全技术有限公司、中能融合智慧科技有限公司、江苏保旺达软件技术有限公司、山石网科通信技术股份有限公司、郑州埃文科技、重庆易阅科技有限公司、浙江木链物联网科技有限公司及其他个人白帽子向 CNVD 提交了 7975 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 4892 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)	2236	2236
三六零数字安全科技集团有限公司	1709	1709
上海交大	947	947
新华三技术有限公司	557	0
北京启明星辰信息安全技术有限公司	538	29
深信服科技股份有限公司	430	0
厦门服云信息科技有限公司	264	0
北京神州绿盟科技有限公司	242	1

安天科技集团股份有 限公司	209	0
北京数字观星科技有 限公司	165	0
北京天融信网络安全 技术有限公司	118	16
杭州安恒信息技术股 份有限公司	104	75
恒安嘉新（北京）科 技股份公司	100	0
阿里云计算有限公司	82	0
中国电信集团系统集 成有限责任公司	59	0
京东科技信息技术有 限公司	37	23
卫士通信息产业股份 有限公司	32	0
杭州迪普科技股份有 限公司	14	0
中国电信股份有限公 司网络安全产品运营 中心	2	2
北京信联数安科技有 限公司	1	1
西安四叶草信息技术 有限公司	1	1
北京升鑫网络科技有 限公司	75	75
博智安全科技股份有 限公司	53	53
河南东方云盾信息技 术有限公司	28	28
奇安星城网络安全运 营服务（长沙）有限 公司	28	28

西门子（中国）有限公司	28	0
上海齐同信息科技有限公司	25	25
北京山石网科信息技术有限公司	24	24
快页信息技术有限公司	24	24
杭州默安科技有限公司	13	13
安徽锋刃信息科技有限公司	10	10
内蒙古洞明科技有限公司	10	10
苏州棱镜七彩信息科技有限公司	9	9
山东新潮信息技术有限公司	8	8
云南联创网安科技有限公司	8	8
湖南轻山信息技术有限公司	7	7
河南灵创电子科技有限公司	5	5
星云博创科技有限公司	4	4
华泰证券股份有限公司	3	3
宁夏凯信特信息科技有限公司	3	3
江苏耘和计算机系统工程有限公司	2	2
上海谋乐网络科技有限公司	2	2
赛尔网络有限公司	2	2

北京华顺信安信息技术有限公司	2	0
任子行网络技术股份有限公司	2	2
墨菲未来科技(北京)有限公司	1	1
亚信科技(成都)有限公司	1	0
杭州美创科技有限公司	1	1
北京网御星云信息技术有限公司	1	1
武汉非尼克斯软件技术有限公司	1	1
北京快手科技有限公司	1	1
山东云天安全技术有限公司	1	1
中能融合智慧科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
山石网科通信技术股份有限公司	1	1
郑州埃文科技	1	1
重庆易阅科技有限公司	1	1
浙江木链物联网科技有限公司	1	1
CNCERT 贵州分中心	1	1
CNCERT 广西分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	2575	2575
报送总计	10813	7975

本周漏洞按类型和厂商统计

本周，CNVD 收录了 351 个漏洞。WEB 应用 151 个，应用程序 89 个，网络设备（交换机、路由器等网络端设备）74 个，操作系统 13 个，智能设备（物联网终端设备）11 个，数据库 10 个，安全产品 3 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	151
应用程序	89
网络设备（交换机、路由器等网络端设备）	74
操作系统	13
智能设备（物联网终端设备）	11
数据库	10
安全产品	3

本周CNVD漏洞数量按影响类型分布

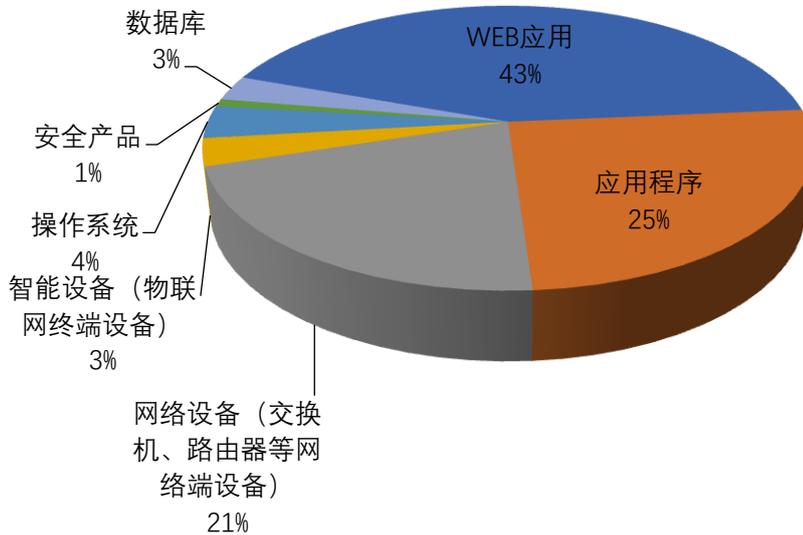


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Tenda、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	Siemens	26	7%

2	Tenda	21	6%
3	Oracle	15	4%
4	DELL	15	4%
5	JR-CMS	13	4%
6	Google	12	4%
7	北京飞易腾科技有限公司	11	3%
8	Adobe	9	3%
9	Telesquare	8	2%
10	其他	221	63%

本周行业漏洞收录情况

本周，CNVD 收录了 56 个电信行业漏洞，11 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Huawei EMUI 拒绝服务漏洞”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/>

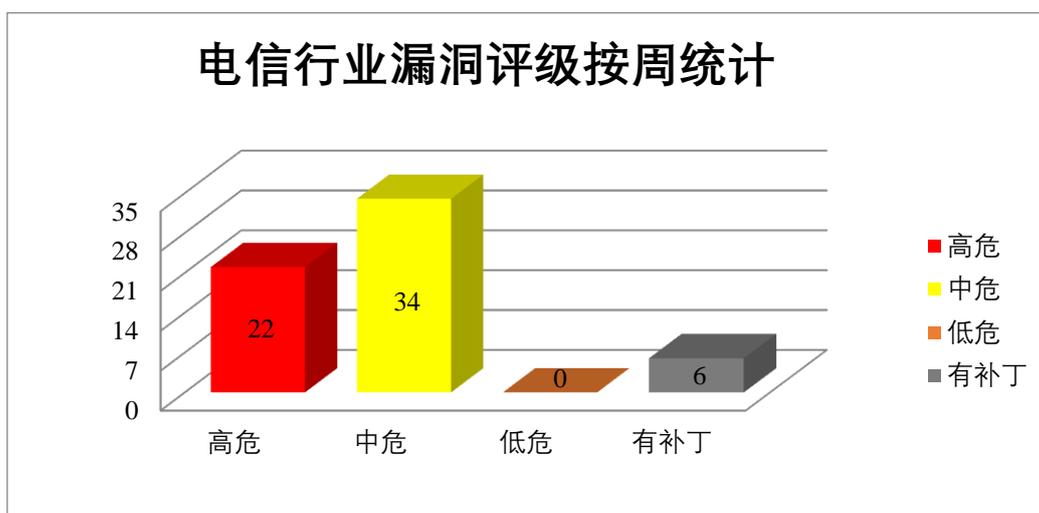


图 3 电信行业漏洞统计

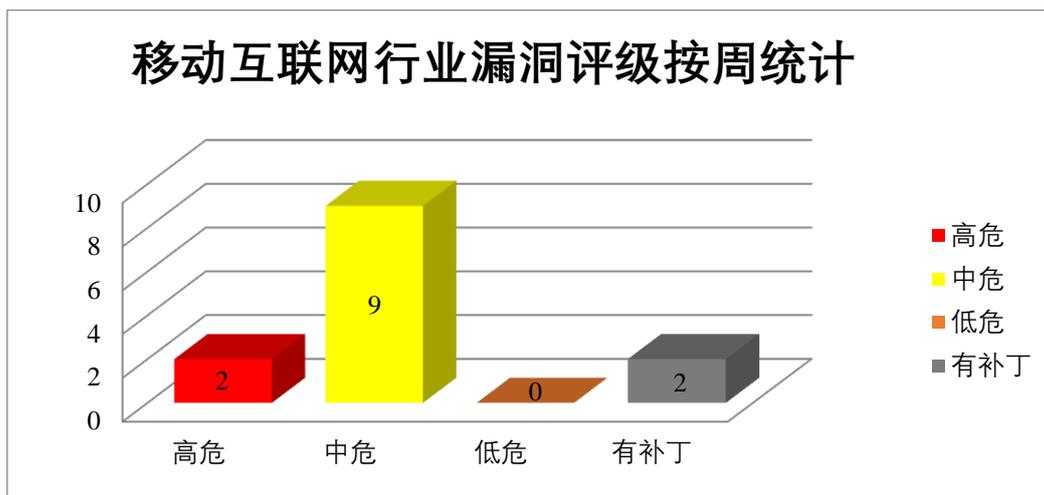


图 4 移动互联网行业漏洞统计

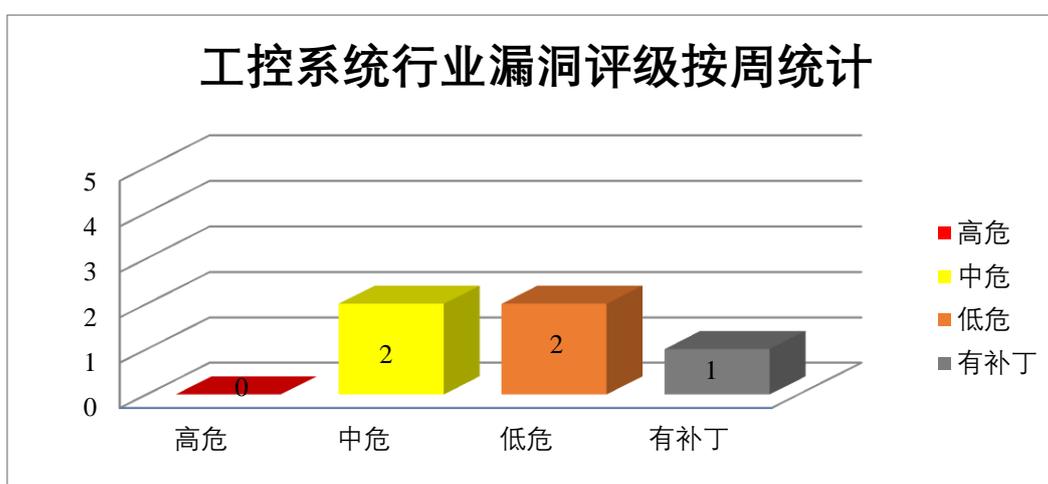


图 5 工控系统行业漏洞统计

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 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，攻击者可利用漏洞导致信息泄露，应用程序拒绝服务，在当前用户的上下文中任意执行代码等。

CNVD 收录的相关漏洞包括：Adobe ColdFusion 缓冲区溢出漏洞、Adobe ColdFusion 路径遍历漏洞（CNVD-2023-08751、CNVD-2023-08754）、Adobe ColdFusion 信任管理问题漏洞、Adobe ColdFusion 信息泄露漏洞、Adobe ColdFusion 输入验证错误漏洞、Adobe ColdFusion XML 外部实体注入漏洞（CNVD-2023-08756、CNVD-2023-08757）。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-2023-08752>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08751>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08755>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08754>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08759>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08758>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08757>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08756>

2、DELL 产品安全漏洞

Dell BIOS 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。Dell Container Storage Modules 是一组模块。旨在提供超出容器存储可用功能的附加功能。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操纵 SMI 导致 SMM 期间的任意写入，使用 SMI 获取 SMRAM 中的任意代码执行等。

CNVD 收录的相关漏洞包括：Dell BIOS 缓冲区溢出漏洞（CNVD-2023-08761、CNVD-2023-08760、CNVD-2023-08766）、Dell BIOS 输入验证错误漏洞（CNVD-2023-08764、CNVD-2023-08763、CNVD-2023-08762、CNVD-2023-08765）、Dell Container Storage Modules 操作系统命令注入漏洞（CNVD-2023-08770）。其中，除“Dell BIOS 输入验证错误漏洞（CNVD-2023-08763）”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-2023-08761>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08760>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08764>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08763>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08762>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08766>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08765>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08770>

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。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：Google Chrome Live Caption 代码执行漏洞、Google Chrome Sign-In 代码执行漏洞、Google Chrome 安全绕过漏洞（CNVD-2023-08259、CNVD-2023-08260、CNVD-2023-08261、CNVD-2023-08277、CNVD-2023-08278、CNVD-2023-08256）。其中，除“Google Chrome 安全绕过漏洞（CNVD-2023-08259、CNVD-2023-08256）”。其中，除“Google Chrome 安全绕过漏洞（CNVD-2023-08259、CNVD-2023-08256）”。

D-2023-08261、CNVD-2023-08277、CNVD-2023-08278）”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-2023-08256>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08257>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08258>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08259>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08260>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08261>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08277>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08278>

4、Oracle 产品安全漏洞

Oracle WebLogic Server 是美国甲骨文（Oracle）公司的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。Oracle E-Business Suite(电子商务套件)是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 Solaris 是一套 UNIX 操作系统。Oracle MySQL 是一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞对关键数据的未授权访问或对所有 Oracle WebLogic Server 可访问数据的完全访问，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 WebLogic Server 信息泄露漏洞（CNVD-2023-08438、CNVD-2023-08437、CNVD-2023-08436）、Oracle E-Business Suite 信息泄露漏洞（CNVD-2023-08435）、Oracle Solaris 拒绝服务漏洞（CNVD-2023-08441、CNVD-2023-08440）、Oracle MySQL Server 拒绝服务漏洞（CNVD-2023-08439）、Oracle MySQL Server Options 组件拒绝服务漏洞。其中“Oracle WebLogic Server 信息泄露漏洞（CNVD-2023-08438、CNVD-2023-08437、CNVD-2023-08436）”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-2023-08438>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08437>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08436>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08435>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08441>
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08440>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08439>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-08445>

5、IBM MQ 输入验证错误漏洞（CNVD-2023-08771）

IBM MQ（IBM WebSphere MQ）是美国国际商业机器（IBM）公司的一款消息传递中间件产品。该产品主要为面向服务的体系结构（SOA）提供可靠的、经过验证的消息传递主干网。本周，IBM MQ 被披露存在输入验证错误漏洞。攻击者可利用该漏洞拒绝 MQTT 通道的服务。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-2023-08771>

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-2023-09114	Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2023-09114）	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://cert-portal.siemens.com/productcert/html/ssa-491245.html
CNVD-2023-09120	Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2023-09120）	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://cert-portal.siemens.com/productcert/html/ssa-491245.html
CNVD-2023-09604	TPCMS 访问控制错误漏洞（CNVD-2023-09604）	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://gitee.com/happy_source/tpcms/issues/I3YNWY
CNVD-2023-09602	XPDF 缓冲区溢出漏洞（CNVD-2023-09602）	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://www.xpdfreader.com/download.html
CNVD-2023-09606	phpwcms 文件上传漏洞（CNVD-2023-09606）	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://github.com/slackero/phpwcms/releases/tag/v1.9.34
CNVD-2023-09611	phpMyAdmin SQL 注入漏洞（CNVD-2023-09611）	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/phpmyadmin/phpmyadmin/commit/ca42395ee4b2936d

			3702524f8fb8bec1e9502bc7
CNVD-2023-09628	phpMyFAQ 跨站脚本漏洞 (CNVD-2023-09628)	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/thorsten/phpMyFAQ/releases/tag/3.1.11
CNVD-2023-09627	IBM Watson Knowledge Catalog 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.ibm.com/support/pages/node/6890729
CNVD-2023-09633	phpMyFAQ 跨站脚本漏洞 (CNVD-2023-09633)	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/thorsten/phpMyFAQ/releases/tag/3.1.11
CNVD-2023-09638	Siemens Solid Edge 越界写入漏洞 (CNVD-2023-09638)	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://cert-portal.siemens.com/productcert/html/ssa-491245.html

小结: 本周, Adobe 产品被披露存在多个漏洞, 攻击者可利用漏洞导致信息泄露, 应用程序拒绝服务, 在当前用户的上下文中任意执行代码等。此外, Dell、Google、Oracle 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限制, 在系统上执行任意代码或导致拒绝服务, 通过操纵 SMI 导致 SMM 期间的任意写入, 使用 SMI 获取 SMRAM 中的任意代码执行。另外, IBM MQ 被披露存在输入验证错误漏洞。攻击者可利用该漏洞拒绝 MQTT 通道的服务。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、Open5GS 拒绝服务漏洞 (CNVD-2023-08774)

验证描述

Open5GS 是一个 5G Core 和 Epc 的 C 语言开源实现, 即 Lte/Nr 网络的核心网络。

Open5GS v2.4.11 版本存在拒绝服务漏洞, 该漏洞源于在 src/smf/pfcp-path.c 中未释放或无法释放已动态分配的堆内存, 攻击者可利用该漏洞通过特制的 pfcp 数据包造成拒绝服务。

验证信息

POC 链接: https://github.com/ToughRunner/Open5gs_bugreport4

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2023-08774>

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. Apple 产品多个漏洞安全风险通告

攻击者可组合利用 CVE-2023-23529 和 CVE-2023-23514 提升权限并逃逸 Safari 沙箱。

参考链接：<https://www.secrss.com/articles/51867>

2. 研究人员在 PyPI Python 包中发现混淆的恶意代码

研究人员已发现 Python 包索引(PyPI)中的四个不同流氓包执行许多恶意操作，包括投放恶意软件、删除 netstat 实用程序和操纵 SSH authorized_keys 文件。

参考链接：<https://thehackernews.com/2023/02/researchers-uncover-obfuscated.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