国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 01 月 30 日-2023 年 02 月 05 日 **2023 年第 5 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 229 个，其中高危漏洞 106 个、中危漏洞 114 个、低危漏洞 9 个。漏洞平均分值为 6.59。本周收录的漏洞中，涉及 0day 漏洞 115 个（占 50%），其中互联网上出现“Lead Management System SQL 注入漏洞（CNVD-2023-05741）、Courier Management System 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 10419 个，与上周（4853 个）环比增加 1.15 倍。

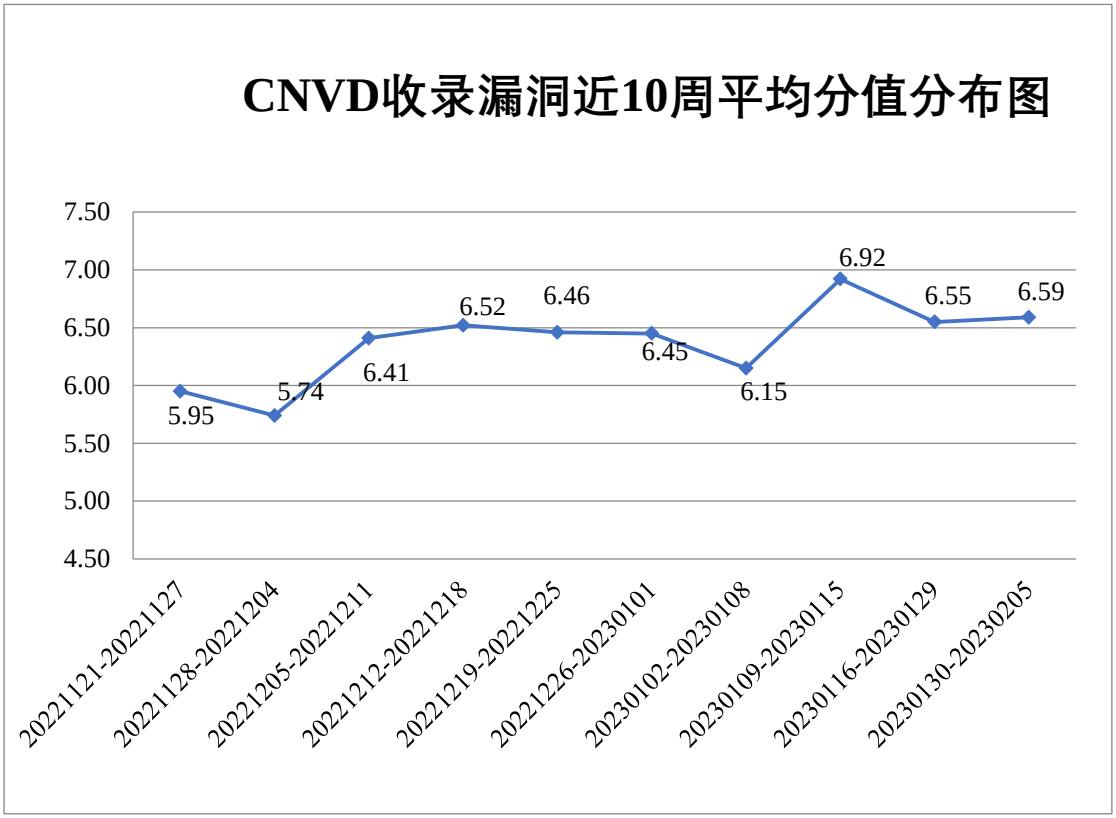

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 起，向基础电信企业通报漏洞事件 41 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 418 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 37 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 96 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：

科大国创云网科技有限公司。

本周，CNVD 发布了《F5 发布 2023 年 2 月季度安全通告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8531

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、安天科技集团股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、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。上海齐同信息科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、苏州棱镜七彩信息科技有限公司、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、山东新潮信息技术有限公司、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、重庆都会信息科技、贵州泰若数字科技有限公司、快页信息技术有限公司、云南联创网安科技有限公司、内蒙古洞明科技有限公司、山东云天安全技术有限公司、赛尔网络有限公司、杭州默安科技有限公司、河南灵创电子科技有限公司、郑州埃文科技、福建省海峡信息技术有限公司、西安秦易信息技术有限公司、江苏金盾检测技术有限公司、江苏保旺达软件技术有限公司、内蒙古中叶信息技术有限责任公司、广西等保安全测评有限公司、重庆易阅科技有限公司及其他个人白帽子向 CNVD 提交了 10419 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）、上海交大和斗象科技（漏洞盒子）、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 8996 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
三六零数字安全科技集团有限公司	5487	5487
斗象科技（漏洞盒子）	1802	1802

奇安信网神（补天平台）	915	915
上海交大	792	792
阿里云计算有限公司	386	0
安天科技集团股份有限公司	328	5
新华三技术有限公司	288	0
北京神州绿盟科技有限公司	205	0
北京启明星辰信息安全技术有限公司	153	17
西安四叶草信息技术有限公司	118	118
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	42	42
北京数字观星科技有限公司	40	0
南京众智维信息科技有限公司	40	40
恒安嘉新（北京）科技股份公司	30	0
杭州迪普科技股份有限公司	30	3
北京安信天行科技有限公司	17	17
北京天融信网络安全技术有限公司	7	6
京东科技信息技术有限公司	4	0
北京知道创宇信息技术有限公司	3	0
中国电信集团系统集成有限责任公司	2	2

浙江大华技术股份有限公司	1	1
上海齐同信息科技有限公司	84	84
奇安星城网络安全运营服务（长沙）有限公司	58	58
苏州棱镜七彩信息科技有限公司	18	18
F5	17	0
北京升鑫网络科技有限公司	17	17
北京山石网科信息技术有限公司	16	16
山东新潮信息技术有限公司	16	16
河南东方云盾信息技术有限公司	15	15
博智安全科技股份有限公司	14	14
重庆都会信息科技	13	13
贵州泰若数字科技有限公司	13	13
快页信息技术有限公司	10	10
云南联创网安科技有限公司	8	8
内蒙古洞明科技有限公司	8	8
中国工商银行股份有限公司软件开发中心	7	7
山东云天安全技术有限公司	5	5
赛尔网络有限公司	5	5
杭州默安科技有限公	3	3

司		
河南灵创电子科技有限公司	3	3
郑州埃文科技	2	2
福建省海峡信息技术有限公司	2	2
西安秦易信息技术有限公司	1	1
江苏金盾检测技术有限公司	1	1
江苏保旺达软件技术有限公司	1	1
内蒙古中叶信息技术有限责任公司	1	1
广西等保安全测评有限公司	1	1
重庆易阅科技有限公司	1	1
CNCERT 宁夏分中心	1	1
CNCERT 广西分中心	1	1
个人	847	847
报送总计	11938	10419

本周漏洞按类型和厂商统计

本周，CNVD 收录了 229 个漏洞。WEB 应用 95 个，应用程序 94 个，网络设备（交换机、路由器等网络端设备）23 个，操作系统 9 个，智能设备（物联网终端设备）7 个，数据库 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	95
应用程序	94
网络设备（交换机、路由器等网络端设备）	23
操作系统	9
智能设备（物联网终端设备）	7
数据库	1

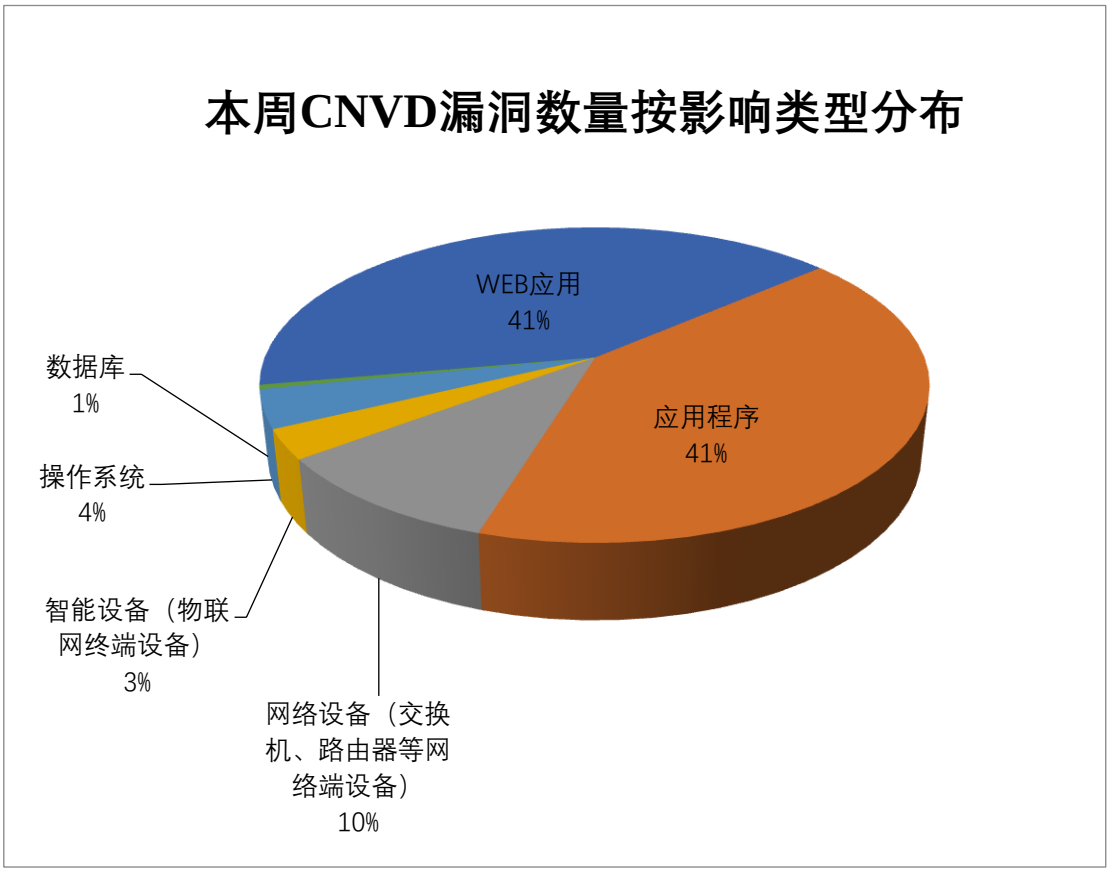

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 F5、Adobe、IBM 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	F5	17	7%
2	Adobe	14	6%
3	IBM	13	6%
4	Mozilla	12	5%
5	Apache	12	5%
6	Oracle	11	5%
7	Mayuri K.	8	4%
8	Online Food Ordering System	6	3%
9	Gas Agency Management System	5	2%
10	其他	131	57%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，10 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“普联技术有限公司 TL-WDR7660 httpProcDataSrv 任意代码执行漏洞、F5 BIG-IP HTTP/2 配置文件拒绝服务漏洞”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/

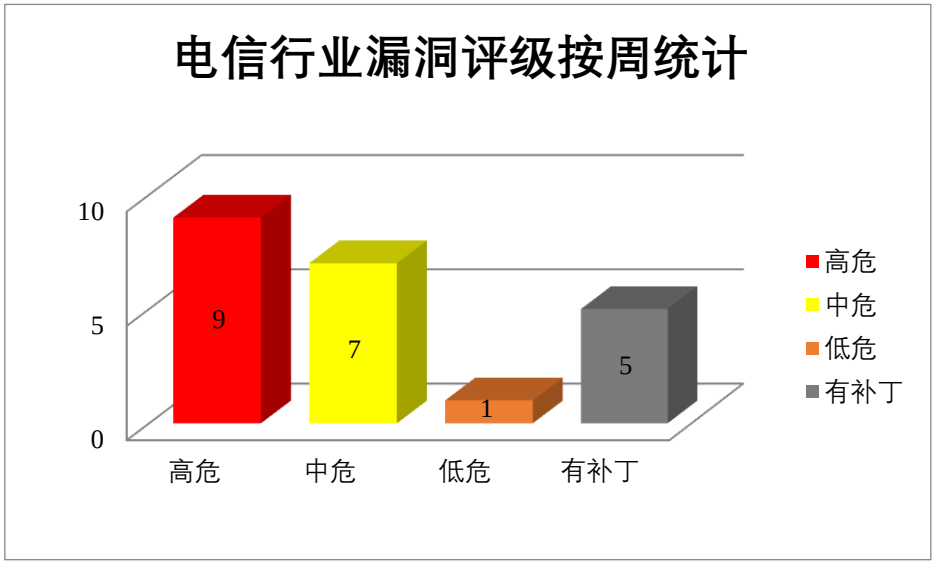

图 3 电信行业漏洞统计

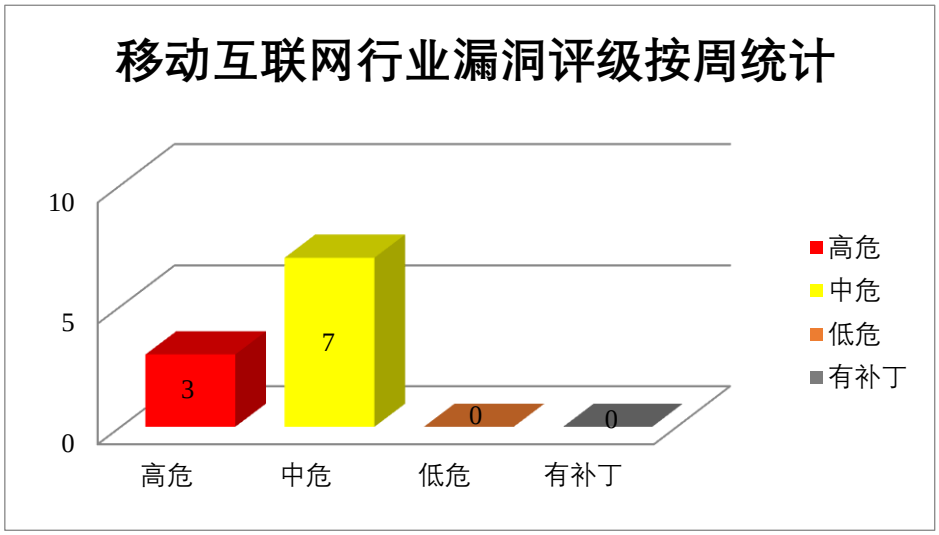

图 4 移动互联网行业漏洞统计

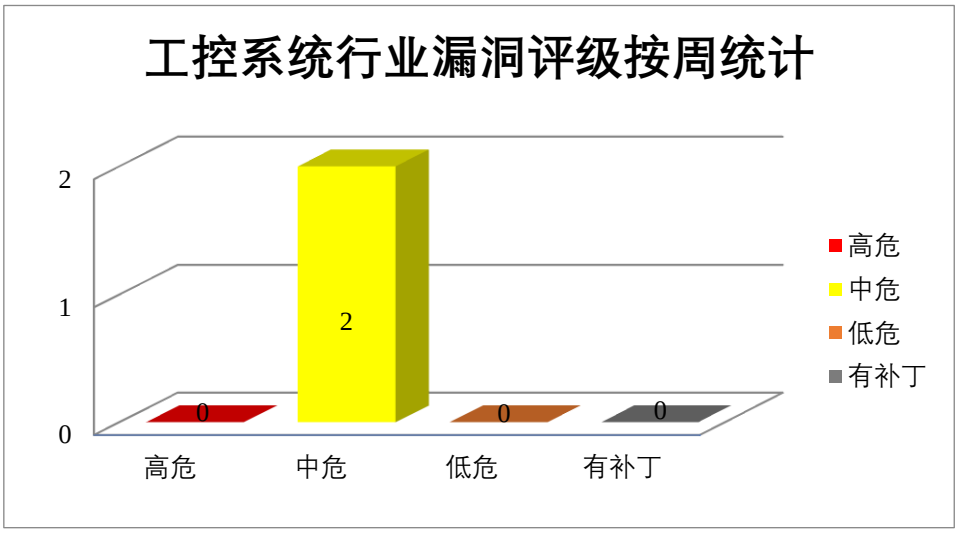

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

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 Spectrum Virtualize 是美国国际商业机器（IBM）公司的一个块存储虚拟化系统。可提高新的和现有存储基础架构的数据价值、安全性和简单性。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期的功能，导致可信会话中的凭证泄露，发送特制的 SQL 语句，查看、添加、修改或删除后端数据库中的信息等。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2023-05240）、IBM Sterling B2B Integrator 权限提升漏洞（CNVD-2023-05239）、IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2023-05238、CNVD-2023-05245）、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2023-05244、CNVD-2023-05241）、IBM Spectrum Virtualize 信息泄露漏洞、IBM Sterling B2B Integrator Standard Edition 跨站脚本漏洞（CNVD-2023-05243）。其中，“IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2023-05240）、IBM Sterling B2B Integrator 权限提升漏洞（CNVD-2023-05239）”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-2023-05240

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05239

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05238

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05243

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05241

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05245

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05244

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05402

2、 Adobe 产品安全漏洞

Adobe InCopy 是美国奥多比（Adobe）公司的一款用于创作的文本编辑软件。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 ASLR 等缓解措施，导致敏感内存泄露，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 InCopy 缓冲区溢出漏洞（CNVD-2023-05227、CNVD-2023-05231）、Adobe InCopy 越界写入漏洞（CNVD-2023-05226、CNVD-2023-05230）、Adobe InCopy 输入验证错误漏洞、Adobe InCopy 释放后使用漏洞、Adobe InCopy 越界读取漏洞（CNVD-2023-05234、CNVD-2023-05225）。其中，除“Adobe InCopy 越界读取漏洞（CNVD-2023-05225、CNVD-2023-05234）、Adobe InCopy 释放后使用漏洞”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-2023-05227

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05226

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05225

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05231

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05230

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05229

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05228

https://www.cnvd.org.cn/flaw/show/CNVD-2023-05234

3、 Apache 产品安全漏洞

Apache Superset 是美国阿帕奇（Apache）基金会的一个数据可视化和数据探索平台。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。Apache James 是美国阿帕奇（Apache）基金会的一个完全用 Java 编写的开源 Smtp 和 Pop3 邮件传输代理和 Nntp 新闻服务器。Apache Calcite 是一个动态数据管理框架，它具备很多典型数据库管理系统的功能，比如 SQL 解析、SQL 校验、SQL 查询优化、SQL 生成以及数据连接查询等。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跨站脚本攻击，提交特殊的请求，可以应用程序上下文执行任意命令等。

CNVD 收录的相关漏洞包括：Apache Superset 跨站脚本漏洞（CNVD-2023-05220、CNVD-2023-05219、CNVD-2023-05218）、Apache Superset 访问控制错误漏洞（CNVD

-2023-05217）、 Apache Airflow 命令注入漏洞（CNVD-2023-05224）、Apache James 信息泄露漏洞、Apache James 授权问题漏洞、Apache Calcite 点击劫持漏洞。其中“Apache Superset跨站请求伪造漏洞、Apache Airflow命令注入漏洞（CNVD-2023-05224）”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-2023-05220
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05219
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05218
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05217
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05224
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05222
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05221
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05273

4、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞能够读取和修改数据，绕过 iframe 沙箱并在任意窗口的上下文中执行任意 JavaScript 代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 安全特征问题漏洞（CNVD-2023-05205、CNVD-2023-05206）、Mozilla Firefox 信任管理问题漏洞（CNVD-2023-05204）、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-05208）、Mozilla Firefox 代码问题漏洞（CNVD-2023-05207）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2023-05212、CNVD-2023-05211）、Mozilla Firefox 竞争条件漏洞。其中，除“Mozilla Firefox 代码问题漏洞（CNVD-2023-05207）”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-2023-05205
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05204
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05208
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05207
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05206
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05212
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05211
https://www.cnvd.org.cn/flaw/show/CNVD-2023-05210

5、Online Food Ordering System 任意文件上传漏洞（CNVD-2023-06523）

Online Food Ordering System 是一个在线食品订购系统。本周，Online Food Orde

ring System 被披露存在文件上传漏洞。攻击者可利用该漏洞上传恶意文件从而远程执行任意代码。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-2023-06523

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-2023-05213	Mozilla Firefox 内存破坏漏洞（CNVD-2023-05213）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/
CNVD-2023-05223	Apache DolphinScheduler 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/r0wqzkjsoq17j6ww381kmpx3jjp9hb6r
CNVD-2023-05233	Adobe InCopy 越界读取漏洞（CNVD-2023-05233）	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/incopy/apsb22-53.html
CNVD-2023-05235	Adobe InCopy 缓冲区溢出漏洞（CNVD-2023-05235）	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/incopy/apsb22-53.html
CNVD-2023-05396	modoboa 跨站请求伪造漏洞（CNVD-2023-05396）	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/modoboa/modoboa/commit/8e14ac93669df4f35fcdebd55dc9d2f0fed3ed48
CNVD-2023-05400	NexusPHP SQL 注入漏洞（CNVD-2023-05400）	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/xiaomlove/nexusphp/releases/tag/v1.7.33
CNVD-2023-05403	D-Link DIR-859 命令注入漏洞	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://us.dlink.com/en/consumer
CNVD-2023-05406	Dell EMC SCG Policy Manager 信任管理问题漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.dell.com/support/kbdoc/en-us/000204995/dsa-2022-273-dell-secure-connect-gateway-policy-mana

			ger-security-update-for-multiple-proprietary-code-vulnerabilities
CNVD-2023-05958	F5 BIG-IP SIP 配置文件拒绝服务漏洞（CNVD-2023-05958）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K34525368
CNVD-2023-05957	F5 BIG-IP SIP 配置文件拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K08182564

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期的功能，导致可信会话中的凭证泄露，发送特制的 SQL 语句，查看、添加、修改或删除后端数据库中的信息等。此外，Adobe、Apache、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过 ASLR 等缓解措施，导致敏感内存泄露，在当前用户的上下文中任意执行代码，读取和修改数据，绕过 iframe 沙箱并在任意窗口的上下文中执行任意 JavaScript 代码等。另外，Online Food Ordering System 被披露存在任意文件上传漏洞。攻击者可利用该漏洞上传恶意文件从而远程执行任意代码。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、Lead Management System SQL 注入漏洞（CNVD-2023-05741）

验证描述

Lead management system 是 Mayuri K.个人开发者的一个潜在客户管理系统。

Lead Management System v1.0 版本存在 SQL 注入漏洞，该漏洞源于 removeBrand.php 中的 id 参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/xiumulty/CVE/blob/main/Lead%20management%20system%20v1.0/sql%20in%20removeBrand.php.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-05741

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. Cisco IOx 和 F5 BIG-IP 产品中发现的新的漏洞

F5 已警告影响 BIG-IP 设备的缺陷可能导致拒绝服务 (DoS) 或任意代码执行。

参考链接：https://thehackernews.com/2023/02/new-high-severity-vulnerabilities.html

2. QNAP 软件存在漏洞，影响近 30000 台设备

据悉，即使远程攻击者没有获得用户交互权限或易受攻击设备上其它权限，也可以轻松利用 CVE-2022-27596 漏洞在受影响的 QNAP 设备上注入恶意代码。

参考链接：https://securityaffairs.com/141705/hacking/qnap-nas-vulnerable-cve-2022-27596.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