国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 04 月 03 日-2023 年 04 月 09 日 **2023 年第 14 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 298 个，其中高危漏洞 116 个、中危漏洞 157 个、低危漏洞 25 个。漏洞平均分值为 6.19。本周收录的漏洞中，涉及 0day 漏洞 251 个（占 84%），其中互联网上出现“Subrion CMS 跨站脚本漏洞（CNVD-2023-23822）、Sourcecodester Logistic Hub Parcel 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漏洞总数 15177 个，与上周（24061 个）环比减少 37%。

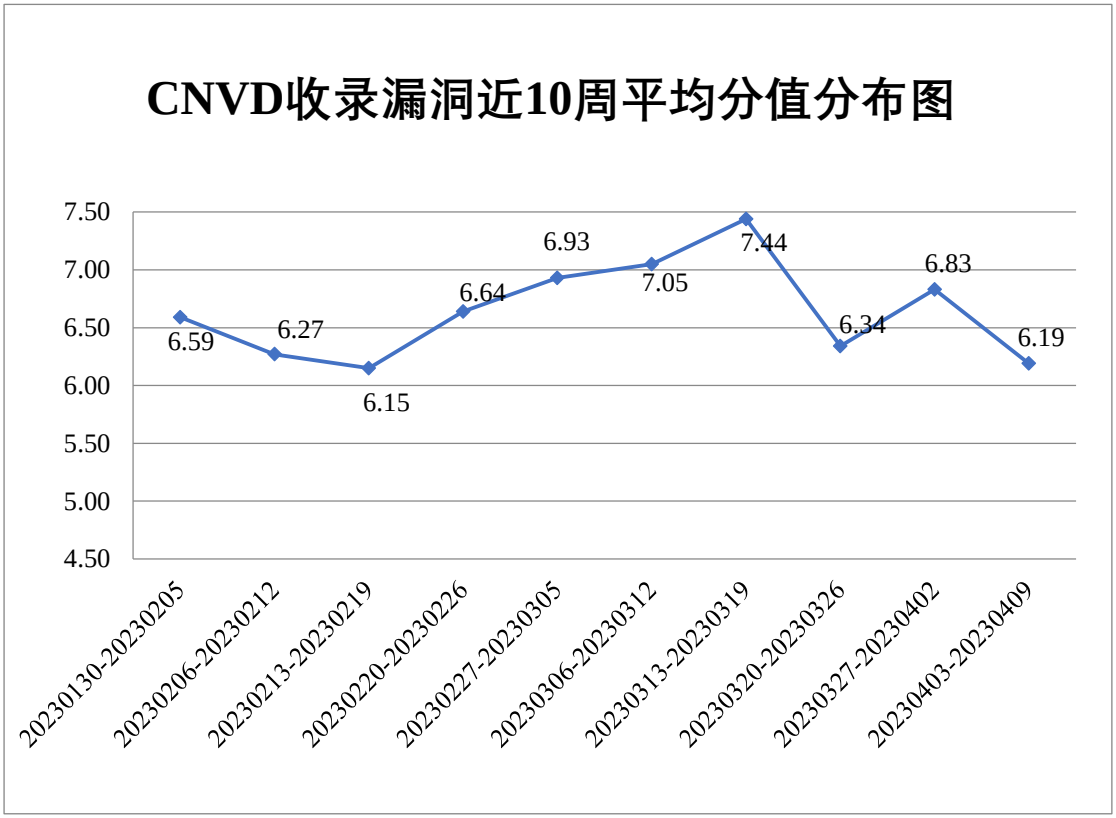

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 63 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 737 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 199 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 98 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：

珠海派诺科技股份有限公司、珠海金山办公软件有限公司、友讯电子设备（上海）有限公司、天津安捷物联科技股份有限公司、深圳维盟科技股份有限公司、深圳市显控科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市和为顺网络技术有限公司、上海金电网安科技有限公司、上海泛微网络科技股份有限公司、上海冰峰计算机网络技术有限公司、北京星网锐捷网络技术有限公司、普联技术有限公司、敬业集团有限公司、合肥奇乐网络科技有限公司、杭州海康威视数字技术股份有限公司、海纳云物联科技有限公司、广州市颖峰信息科技有限公司、广州红帆科技有限公司、帆软软件有限公司、成都成电医星数字健康软件有限公司、畅捷通信息技术股份有限公司、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、北京万户网络技术有限公司、北京通达信科科技有限公司、安科瑞电气股份有限公司、安徽青柿信息科技有限公司和 ZZCMS。

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、北京神州绿盟科技有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。快页信息技术有限公司、北京升鑫网络科技有限公司、博智安全科技股份有限公司、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、河南信安世纪科技有限公司、杭州美创科技有限公司、山东鼎夏智能科技有限公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、内蒙古中叶信息技术有限责任公司、汇安云（山东）信息科技有限公司、重庆都会信息科技、广州安亿信软件科技有限公司、云南联创网安科技有限公司、湖南轻山信息技术有限公司、杭州默安科技有限公司、北京珞安科技有限责任公司、合肥梆梆信息科技有限公司、福建省海峡信息技术有限公司、江苏君立华域信息安全技术股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京远禾科技有限公司、思而听网络科技有限公司、河南灵创电子科技有限公司、北京华顺信安信息技术有限公司、联想集团、任子行网络技

术股份有限公司及其他个人白帽子向 CNVD 提交了 15177 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）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 13896 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）	9289	9289
斗象科技（漏洞盒子）	2923	2923
三六零数字安全科技集团有限公司	1268	1268
深信服科技股份有限公司	835	0
上海交大	416	416
新华三技术有限公司	275	0
安天科技集团股份有限公司	260	0
北京神州绿盟科技有限公司	202	0
阿里云计算有限公司	193	0
北京数字观星科技有限公司	172	0
北京启明星辰信息安全技术有限公司	101	1
中国电信集团系统集成有限责任公司	25	0
远江盛邦（北京）网络安全科技股份有限公司	19	19
杭州迪普科技股份有限公司	13	0
京东科技信息技术有限公司	2	2
快页信息技术有限公司	156	156
北京升鑫网络科技有	148	148

限公司		
博智安全科技股份有限公司	50	50
北京山石网科信息技术有限公司	41	41
上海齐同信息科技有限公司	18	18
河南信安世纪科技有限公司	15	15
杭州美创科技有限公司	14	14
山东鼎夏智能科技有限公司	9	9
安徽锋刃信息科技有限公司	8	8
河南东方云盾信息技术有限公司	6	6
内蒙古中叶信息技术有限责任公司	4	4
汇安云（山东）信息科技有限公司	3	3
重庆都会信息科技	3	3
广州安亿信软件科技有限公司	2	2
云南联创网安科技有限公司	2	2
湖南轻山信息技术有限公司	2	2
杭州默安科技有限公司	2	2
北京珞安科技有限责任公司	1	1
合肥梆梆信息科技有限公司	1	1
福建省海峡信息技术	1	1

有限公司		
江苏君立华域信息安全技术股份有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
北京远禾科技有限公司	1	1
思而听网络科技有限公司	1	1
河南灵创电子科技有限公司	1	1
北京华顺信安信息技术有限公司	277	0
联想集团	2	2
任子行网络技术股份有限公司	1	1
个人	765	765
报送总计	17529	15177

本周漏洞按类型和厂商统计

本周，CNVD 收录了 298 个漏洞。WEB 应用 155 个，应用程序 55 个，网络设备（交换机、路由器等网络端设备）47 个，智能设备（物联网终端设备）30 个，安全产品 5 个，数据库 4 个，操作系统 2 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	155
应用程序	55
网络设备（交换机、路由器等网络端设备）	47
智能设备（物联网终端设备）	30
安全产品	5
数据库	4
操作系统	2

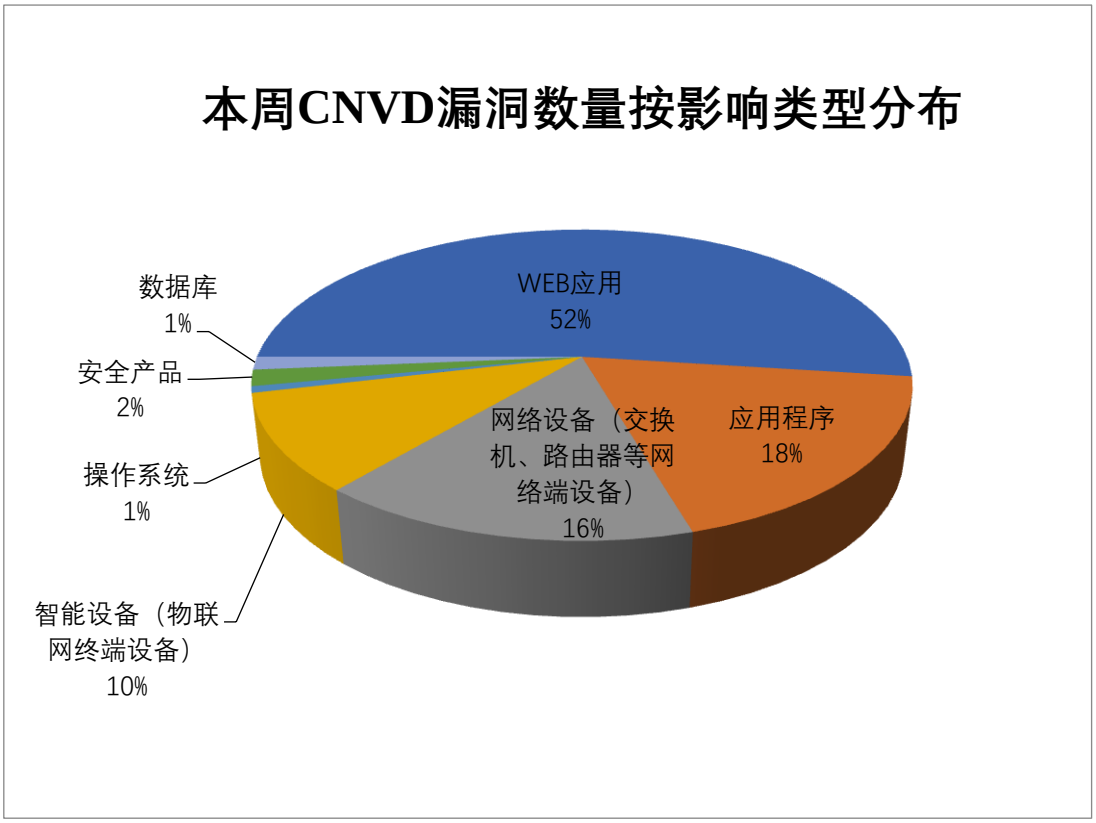

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apache、Delta Electronics、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	Apache	13	4%
2	Delta Electronics	13	4%
3	Google	12	4%
4	松下电器（中国）有限公司	10	3%
5	Foxit	10	3%
6	北京百卓网络技术有限公司	8	3%
7	TOTOLINK	7	3%
8	深圳市必联电子有限公司	6	2%
9	富士施乐（中国）有限公司	5	2%
10	其他	214	72%

本周行业漏洞收录情况

本周，CNVD 收录了 36 个电信行业漏洞，16 个移动互联网行业漏洞。其中，“

Google Android 缓冲区溢出漏洞（CNVD-2023-25101）”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/

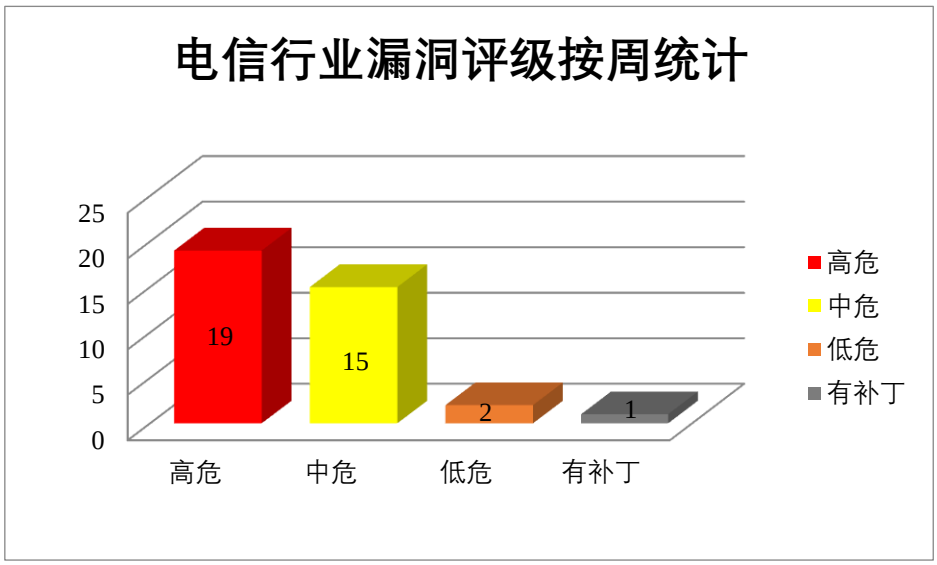

图 3 电信行业漏洞统计

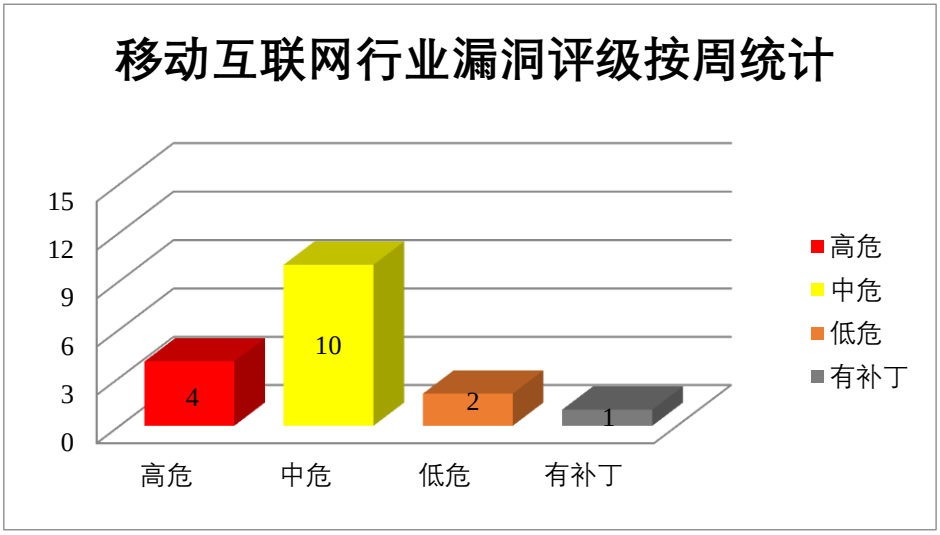

图 4 移动互联网行业漏洞统计

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 Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Pixel 是美国谷歌（Google）公司的一款智能手机。Google Android 是美国谷歌（Google）公司的

一套以 Linux 为基础的开源操作系统。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，通过精心设计的 HTML 页面潜在地利用堆损坏。

CNVD 收录的相关漏洞包括：Google Chrome ANGLE 越界读取漏洞、Google Chrome ANGLE 内存错误引用漏洞（CNVD-2023-23573）、Google Pixel bta_av_co.cc 文件缓冲区溢出漏洞、Google Chrome 越界访问漏洞、Google Pixel ble_scanner_hci_interface.cc 文件缓冲区溢出漏洞、Google Chrome Web Payments API 组件代码问题漏洞、Google Chrome Navigation 组件代码问题漏洞、Google Android 缓冲区溢出漏洞（CNVD-2023-25101）。其中“Google Chrome ANGLE 越界读取漏洞、Google Chrome ANGLE 内存错误引用漏洞（CNVD-2023-23573）、Google Chrome 越界访问漏洞、Google Android 缓冲区溢出漏洞（CNVD-2023-25101）”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-2023-23574
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23573
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23572
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23819
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23818
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23821
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23820
https://www.cnvd.org.cn/flaw/show/CNVD-2023-25101

2、 Apache 产品安全漏洞

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 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 Kafka 是美国阿帕奇（Apache）基金会的一套开源的分布式流媒体平台。该平台能够获取实时数据，用于构建对数据流的变化进行实时反应的应用程序。Apache ShenYu 是美国阿帕奇（Apache）基金会的一个异步的，高性能的，跨语言的，响应式的 API 网关。Apache Commons FileUpload 是美国阿帕奇（Apache）基金会的一个可将文件上传到 Servlet 和 Web 应用程序的软件包。Apache NiFi 是美国阿帕奇（Apache）基金会的一套数据处理和分发系统。该系统主要用于数据路由、转换和系统中介逻辑。Apache Fineract 是美国阿帕奇（Apache）基金会的一套开源数字金融服务平台。该平台能够为用户提供数据管理、贷款和储蓄投资组合管理以及实时财务数据等功能。Apache Archiva 是美国阿帕奇（Apache）基金会的一套用于管理一个或多个远程存储的软件。该软件提供远程 Repository 代理、基于角色的安全访问管理和使用情况报告等功能。本周，上述产品被披露

存在多个漏洞，攻击者可利用漏洞获取敏感信息，在受害者的系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Apache Dubbo 代码问题漏洞（CNVD-2023-23551）、Apache Airflow 信息泄露漏洞（CNVD-2023-23550）、Apache Kafka 代码问题漏洞（CNVD-2023-23554）、Apache ShenYu 授权问题漏洞（CNVD-2023-23553）、Apache Commons FileUpload 拒绝服务漏洞（CNVD-2023-23552）、Apache NiFi XML 外部实体注入漏洞（CNVD-2023-23555）、Apache Fineract SQL 注入漏洞（CNVD-2023-23557）、Apache Archiva 跨站脚本漏洞（CNVD-2023-23556）。其中，除“Apache Airflow 信息泄露漏洞（CNVD-2023-23550）、Apache Fineract SQL 注入漏洞（CNVD-2023-23557）、Apache Archiva 跨站脚本漏洞（CNVD-2023-23556）”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-2023-23551
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23550
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23554
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23553
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23552
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23555
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23557
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23556

3、Foxit 产品安全漏洞

Foxit PDF Editor 是中国福昕（Foxit）公司的一款 PDF 编辑器。Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 阅读器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Editor 远程代码执行漏洞（CNVD-2023-23560、CNVD-2023-23563）、Foxit PDF Reader 远程代码执行漏洞（CNVD-2023-23565、CNVD-2023-23566、CNVD-2023-23568、CNVD-2023-23567、CNVD-2023-23570、CNVD-2023-23569）。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-2023-23560
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23563
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23565
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23566
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23568
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23567
https://www.cnvd.org.cn/flaw/show/CNVD-2023-23570

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23569

4、Delta Electronics 产品安全漏洞

Delta Electronics InfraSuite Device Master 是 Delta Electronics 的用于简化和自动化关键设备监控的设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取本地文件、公开明文凭据并升级权限，远程执行代码等。

CNVD 收录的相关漏洞包括：Delta Electronics InfraSuite Device Master 路径遍历漏洞（CNVD-2023-23884、CNVD-2023-23890）、Delta Electronics InfraSuite Device Master 反序列化漏洞（CNVD-2023-23883、CNVD-2023-23887）、Delta Electronics InfraSuite Device Master 认证错误漏洞、Delta Electronics InfraSuite Device Master 身份验证错误漏洞、Delta Electronics InfraSuite Device Master 命令注入漏洞、Delta Electronics InfraSuite Device Master 访问控制错误漏洞（CNVD-2023-23889）。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-2023-23884

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23883

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23887

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23885

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23892

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23891

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23890

https://www.cnvd.org.cn/flaw/show/CNVD-2023-23889

5、Home Owners Collection Management System 文件上传漏洞

Home Owners Collection Management System 是一个业主收款管理系统。本周，Home Owners Collection Management System 被披露存在文件上传漏洞。攻击者可利用该漏洞通过精心制作的 PHP 文件执行任意代码。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-2023-25099

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

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-2023-23560	Foxit PDF Editor 远程代码执行漏洞（CNVD-2023-23560）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html

CNVD-2023-23565	Foxit PDF Reader 远程代码执行漏洞（CNVD-2023-23565）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html
CNVD-2023-23884	Delta Electronics InfraSuite Device Master 路径遍历漏洞（CNVD-2023-23884）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/
CNVD-2023-23885	Delta Electronics InfraSuite Device Master 认证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/
CNVD-2023-23889	Delta Electronics InfraSuite Device Master 访问控制错误漏洞（CNVD-2023-23889）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/
CNVD-2023-23891	Delta Electronics InfraSuite Device Master 命令注入漏洞	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.deltaww.com/
CNVD-2023-23892	Delta Electronics InfraSuite Device Master 身份验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/
CNVD-2023-23573	Google Chrome ANGLE 内存错误引用漏洞（CNVD-2023-23573）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html
CNVD-2023-23574	Google Chrome ANGLE 越界读取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html
CNVD-2023-23551	Apache Dubbo 代码问题漏洞（CNVD-2023-23551）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/8h6zscfzj482z512d2v5ft63hdhzm0cb

小结：本周，Google 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，通过精心设计的 HTML 页面潜在地利用堆损坏。此外，Apache、Foxit、Delta Electronics 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在受害者的系统上执行任意代码等。另外，Home Owners Collection Management System 被披露存在文件上传漏洞。攻击者可利用该漏洞通过精心制作的 PHP 文件执行任意代码。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、Subrion CMS 跨站脚本漏洞（CNVD-2023-23822）

验证描述

Subrion CMS 是一套基于 PHP 的内容管理系统（CMS）。该系统可被集成到网站，并支持多种扩展插件等。

Subrion CMS 4.2.1 版本及之前版本存在跨站脚本漏洞，该漏洞源于通过 SGV 文件创建管理帐户的页面功能中缺少对用户提供的数据和输出的数据校验过滤。攻击者可利用该漏洞在客户端执行 JavaScript 代码。

验证信息

POC 链接：https://github.com/intelliants/subrion/issues/890

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-23822

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. 身份验证厂商 OCR Labs 数据泄露，危及大量银行客户

据 Cybernews 报道，全球知名数字身份验证工具提供商 OCR Labs 近日曝出敏感数据泄露事件，导致较多银行和政府客户面临安全风险。

参考链接：https://www.secrss.com/articles/53466

2. 黑客使用 Rilide 浏览器扩展绕过 2FA，窃取加密货币

安全研究人员发现了一种名为 Rilide 的新恶意浏览器扩展，该扩展针对基于 Chromium 的产品，如 Google Chrome、Brave、Opera 和 Microsoft Edge。

参考链接：https://www.bleepingcomputer.com/news/security/hackers-use-rilide-browser-extension-to-bypass-2fa-steal-crypto/

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