国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 07 月 10 日-2023 年 07 月 16 日 **2023 年第 28 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 326 个，其中高危漏洞 152 个、中危漏洞 156 个、低危漏洞 18 个。漏洞平均分值为 6.42。本周收录的漏洞中，涉及 0day 漏洞 249 个（占 76%），其中互联网上出现“Milesight UR32L firewall_handler_set 函数缓冲区溢出漏洞（CNVD-2023-55360、CNVD-2023-55361）”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 11081 个，与上周（7156 个）环比增加 55%。

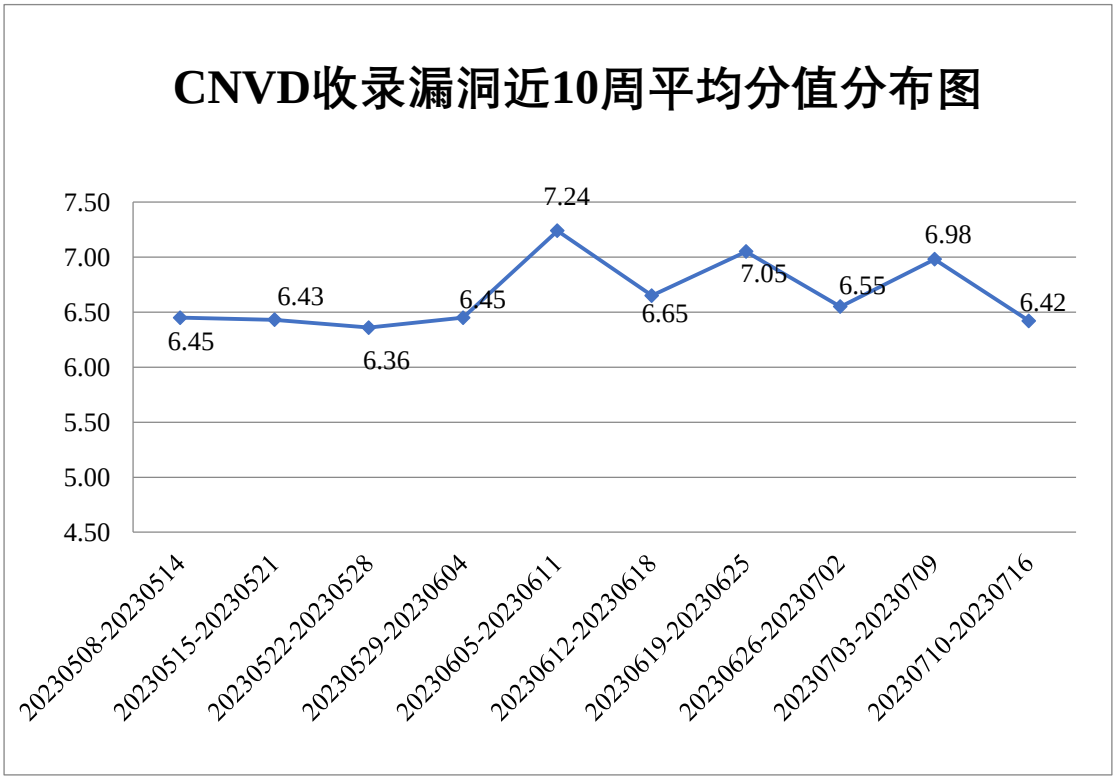

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 14 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 698 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 49 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：

珠海奔图电子有限公司、重庆远秋科技股份有限公司、中科医创科技有限公司、郑州木云电子科技有限公司、浙江中控技术股份有限公司、浙江环鑫信息技术有限公司、云南七丹药业股份有限公司、远孚物流集团有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永安行科技股份有限公司、研华科技（中国）有限公司、新开普电子股份有限公司、小佩网络科技（上海）有限公司、武汉理工光科股份有限公司、微医贝联（上海）信息科技有限公司、微鲸科技有限公司、天津卓朗科技发展有限公司、天津塘沽瓦德斯特阀门有限公司、天津神州浩天科技有限公司、天津黑核科技有限公司、天地伟业技术有限公司、深圳智慧园区信息技术有限公司、深圳找靓机网络技术发展有限责任公司、深圳市智美达科技股份有限公司、深圳市粤电新能源技术有限公司、深圳市科力锐科技有限公司、深圳市吉祥腾达科技有限公司、深圳市东宝信息技术有限公司、深圳市百家骏网络科技有限公司、深圳市安之源电子有限公司、上海卓卓网络科技有限公司、上海卓盟信息科技有限公司、上海鹰谷信息科技有限公司、上海昕想智能科技有限公司、上海思顶信息科技有限公司、上海荃路软件开发工作室、上海寰创通信科技股份有限公司、上海汉得信息技术股份有限公司、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、上海保利物业酒店管理集团有限公司、山西硕成教育培训学校股份有限公司、山东中创软件商用中间件股份有限公司、山东博硕自动化技术有限公司、厦门永陞科技有限公司、厦门同迈科技有限公司、瑞斯康达科技发展股份有限公司、千城智联（上海）网络科技有限公司、普元信息技术股份有限公司、普联技术有限公司、迈普通信技术股份有限公司、朗诗寓商业管理（深圳）有限公司、锦程国际物流发展有限公司、金蝶软件（中国）有限公司、金碧智慧生活科技（深圳）有限公司、江西元聚网络科技有限公司、江西铭软科技有限公司、江西金手指人力资源集团有限公司、江西赣贸数字科技集团有限公司、江苏新华日报财经传媒有限公司、江苏凤凰画材科技股份有限公司、佳能（中国）有限公司、济南时刻信息技术有限公司、吉翁电子（深圳）有限公司、惠尔丰信息系统有限公司、湖南翱云网络科技有限公司、红门智能科技股份有限公司、杭州叙简科技股份有限公司、杭州新中大科技股份有限公司、杭州万为科技有限责任公司、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、杭州安恒信息技术股份有限公司、汉王科技股份有限公司、贵州向雪怀酒业有限公

司、广州粤建三和软件股份有限公司、广州远智教育科技有限公司、广州思迈特软件有限公司、广州市保伦电子有限公司、飞天下载系统、东莞市东城飞飞网络科技经营部、滴咚个游科技（广东）有限公司、成都星锐蓝海网络科技有限公司、畅捷通信息技术股份有限公司、北京中百信软件技术有限公司、北京亚鸿世纪科技发展有限公司、北京星网锐捷网络技术有限公司、北京小熊博望科技有限公司、北京万讯博通科技发展有限公司、北京通达信科科技有限公司、北京环球启航教育科技有限公司、北京花千树文化发展有限公司、北京宏景世纪软件股份有限公司、北京格林威尔科技发展有限公司、北京百卓网络技术有限公司、奥琦玮信息科技（北京）有限公司、安翼物联网（南京）有限公司、安美世纪（北京）科技有限公司、安徽协达软件科技有限公司、安徽青柿信息科技有限公司、安达康股份有限公司、爱普生（中国）有限公司、SEMCMS、nginxWebUI 和 NETGEAR。

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、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、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。内蒙古中叶信息技术有限责任公司、河南东方云盾信息技术有限公司、重庆电信系统集成有限公司、杭州美创科技有限公司、安徽锋刃信息科技有限公司、联想集团、快页信息技术有限公司、赛尔网络有限公司、北京赛博昆仑科技有限公司、平安银河实验室、北京六方云信息技术有限公司、河南信安世纪科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、星云博创科技有限公司、信息产业信息安全测评中心、江苏晟晖信息科技有限公司、国网上海市电力公司、中国工商银行股份有限公司软件开发中心、河南悦海数安科技有限公司、河南省鼎信信息安全等级测评有限公司、亚信科技（成都）有限公司、重庆易阅科技有限公司、工业和信息化部电子第五研究所、宁夏凯信特信息科技有限公司、中国航天系统科学与工程研究院、杭州默安科技有限公司、上海市信息安全测评认证中心、北京微步在线科技有限公司、江西诚韬科技有限公司、浙江木链物联网科技有限公司、广西网信信息技术有限公司及其他个人白帽子向 CNVD 提交了 11081 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）、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 9131 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）	4159	4159
奇安信网神（补天平台）	3722	3722

新华三技术有限公司	905	0
北京天融信网络安全技术有限公司	624	9
上海交大	652	652
三六零数字安全科技集团有限公司	598	598
北京神州绿盟科技有限公司	407	17
北京启明星辰信息安全技术有限公司	390	19
深信服科技股份有限公司	350	0
安天科技集团股份有限公司	324	0
北京长亭科技有限公司	254	10
阿里云计算有限公司	192	3
北京数字观星科技有限公司	141	0
天津市国瑞数码安全系统股份有限公司	118	0
厦门服云信息科技有限公司	105	0
北京知道创宇信息技术有限公司	52	0
远江盛邦（北京）网络安全科技股份有限公司	27	27
杭州迪普科技股份有限公司	14	0
京东科技信息技术有限公司	11	0
北京智游网安科技有限公司	4	4
卫士通信息产业股份	3	3

有限公司		
华为技术有限公司	3	3
西安四叶草信息技术有限公司	2	2
内蒙古奥创科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
杭州安恒信息技术股份有限公司	1	1
南京铱迅信息技术股份有限公司	1	1
内蒙古中叶信息技术有限责任公司	134	134
河南东方云盾信息技术有限公司	52	52
重庆电信系统集成有限公司	47	47
杭州美创科技有限公司	45	45
西门子（中国）有限公司	25	0
安徽锋刃信息科技有限公司	25	25
联想集团	20	20
快页信息技术有限公司	15	15
赛尔网络有限公司	8	8
北京赛博昆仑科技有限公司	7	7
平安银河实验室	7	7
北京六方云信息技术有限公司	6	6
河南信安世纪科技有	6	6

限公司		
奇安星城网络安全运营服务（长沙）有限公司	5	5
星云博创科技有限公司	4	4
信息产业信息安全测评中心	3	3
江苏晟晖信息科技有限公司	3	3
国网上海市电力公司	2	2
中国工商银行股份有限公司软件开发中心	2	2
河南悦海数安科技有限公司	2	2
河南省鼎信信息安全等级测评有限公司	2	2
亚信科技（成都）有限公司	1	1
重庆易阅科技有限公司	1	1
工业和信息化部电子第五研究所	1	1
宁夏凯信特信息科技有限公司	1	1
中国航天系统科学与工程研究院	1	1
杭州默安科技有限公司	1	1
上海市信息安全测评认证中心	1	1
北京微步在线科技有限公司	1	1
江西诚韬科技有限公司	1	1

浙江木链物联网科技有限公司	1	1
广西网信信息技术有限公司	1	1
个人	1443	1443
报送总计	14935	11081

本周漏洞按类型和厂商统计

本周，CNVD 收录了 326 个漏洞。WEB 应用 162 个，应用程序 63 个，网络设备（交换机、路由器等网络端设备）58 个，操作系统 25 个，智能设备（物联网终端设备）18 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	162
应用程序	63
网络设备（交换机、路由器等网络端设备）	58
操作系统	25
智能设备（物联网终端设备）	18

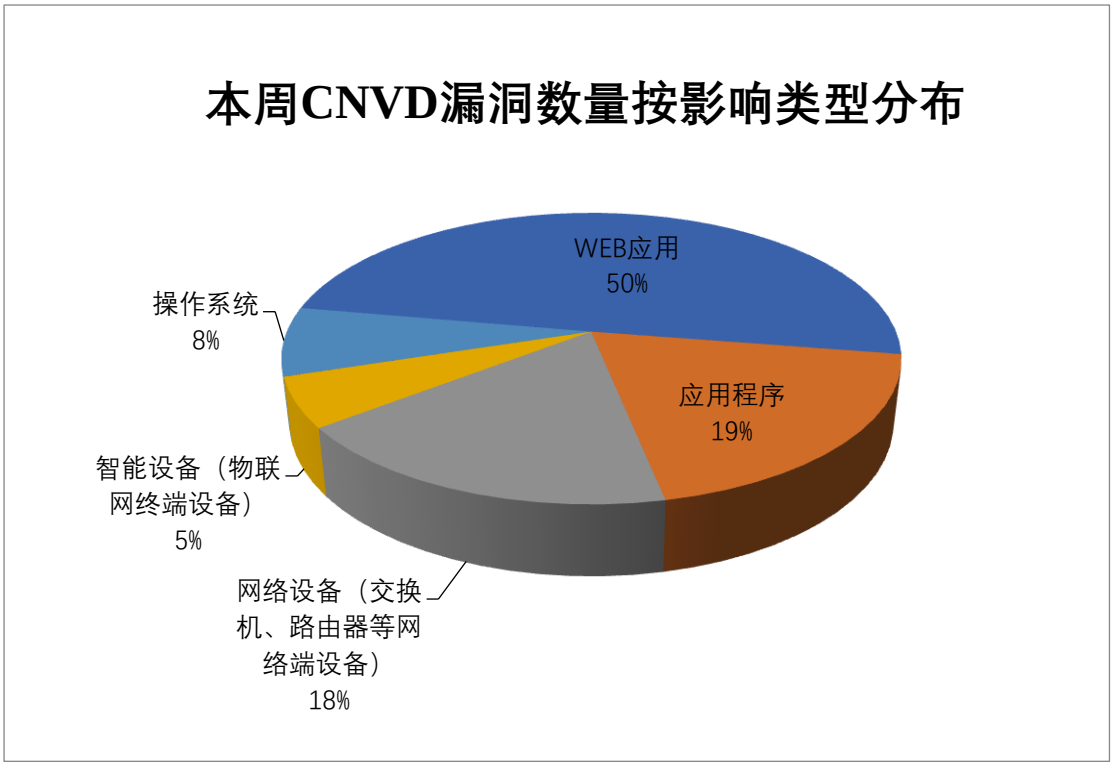

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、D-Link、Mattermost 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	20	6%
2	D-Link	14	5%
3	Mattermost	11	3%
4	Apache	11	3%
5	北京百卓网络技术有限公司	10	3%
6	Adobe	10	3%
7	安美世纪（北京）科技有限公司	9	3%
8	Mozilla	9	3%
9	北京米尔伟业科技有限公司	7	2%
10	其他	225	69%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，38 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Google Android 代码执行漏洞（CNVD-2023-55382）、Schneider Electric EcoStruxure Foxboro DCS 缓冲区溢出漏洞”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/

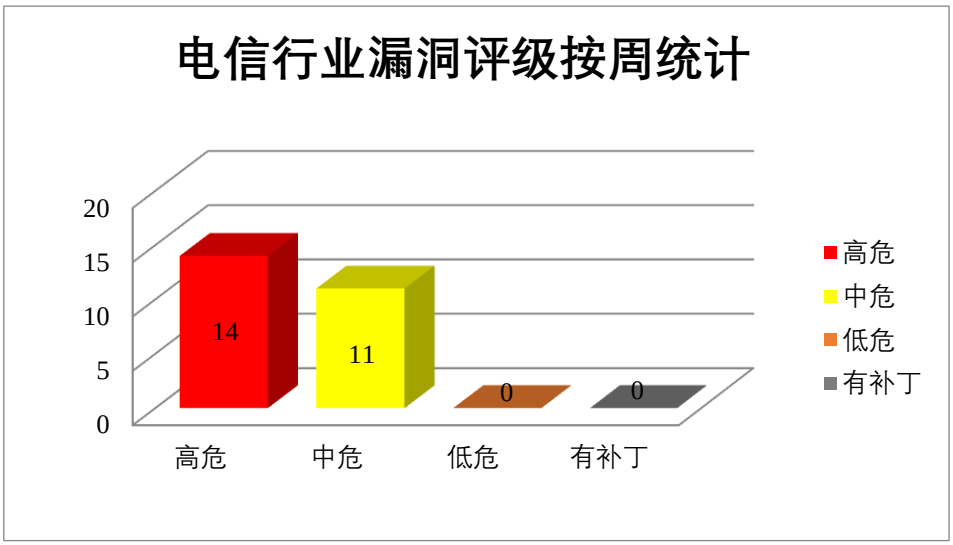

图 3 电信行业漏洞统计

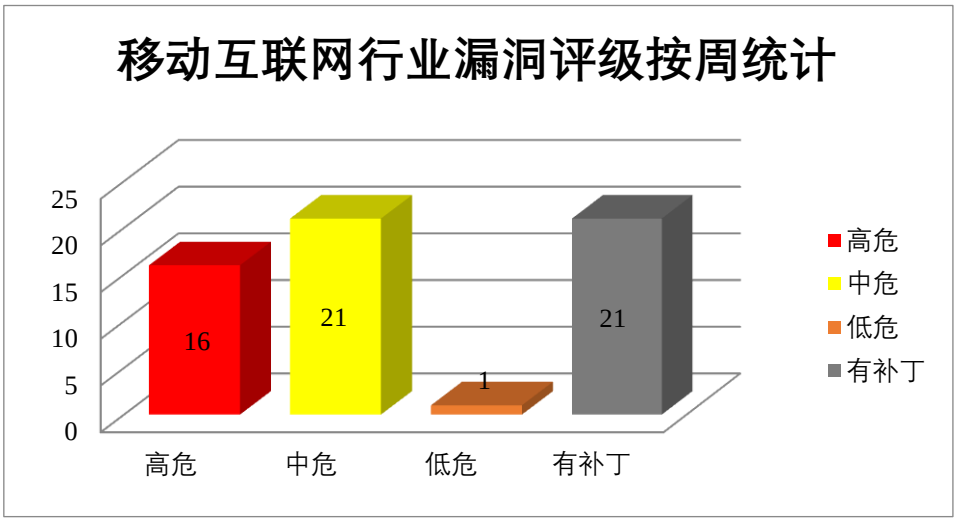

图 4 移动互联网行业漏洞统计

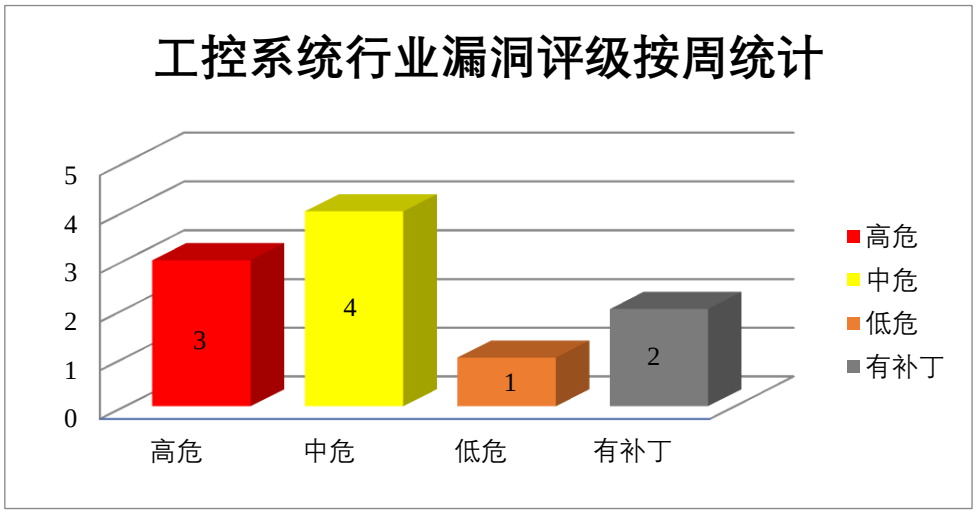

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。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用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2023-55032、CNVD-2023-55035、CNVD-2023-55034、CNVD-2023-55033、CNVD-2023-55038、CNVD-2023-55037、CNVD-2023-55036）、Adobe Acrobat Reader 输入验证错

误漏洞（CNVD-2023-55030）。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-2023-55032
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55030
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55035
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55034
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55033
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55038
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55037
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55036

2、 Mozilla 产品安全漏洞

Mozilla Firefox ESR 是美国 Mozilla 基金会的 Firefox（Web 浏览器）的一个延长支持版本。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，攻击者可利用漏洞使应用程序崩溃或以应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox ESR 缓冲区溢出漏洞（CNVD-2023-55348）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-55349、CNVD-2023-55351、CNVD-2023-55350、CNVD-2023-55354）、Mozilla Firefox 代码问题漏洞（CNVD-2023-55355）、Mozilla Firefox ESR 拒绝服务漏洞（CNVD-2023-55353）、Mozilla Firefox 资源管理错误漏洞（CNVD-2023-55356）。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-2023-55348
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55349
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55351
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55350
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55355
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55354
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55353
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55356

3、 Apache 产品安全漏洞

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 Airflow Hive Provider 是一个使用 SQL 读取、写入和管理分布式存储中的大型数据集的工具包。Apache StreamPipes 是美国阿帕奇（Apache）基金

会的一个自助式（工业）物联网工具箱，使非技术用户能够连接、分析和探索 IIoT 数据流。Apache Struts 是美国阿帕奇（Apache）基金会的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。Apache Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。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，提升权限，在系统上执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Apache Hive Provider 代码执行漏洞、Apache Airflow JDBC Provider 代码执行漏洞、Apache Airflow ODBC Provider 远程代码执行漏洞、Apache StreamPipes 权限提升漏洞、Apache Airflow 信息泄露漏洞（CNVD-2023-55401）、Apache Struts 拒绝服务漏洞（CNVD-2023-55422、CNVD-2023-55432）、Apache Traffic Server 拒绝服务漏洞（CNVD-2023-55453）。其中，除“Apache Traffic Server 拒绝服务漏洞（CNVD-2023-55453）”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-2023-55392
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55393
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55394
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55396
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55401
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55422
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55432
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55453

4、Google 产品安全漏洞

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，攻击者可利用漏洞获取敏感信息，提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-55374、CNVD-2023-55375、CNVD-2023-55377、CNVD-2023-55378、CNVD-2023-55380、CNVD-2023-55381）、Google Android 代码执行漏洞（CNVD-2023-55382）、Google Android 信息泄露漏洞（CNVD-2023-55376）。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-2023-55374
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55375
https://www.cnvd.org.cn/flaw/show/CNVD-2023-55376

https://www.cnvd.org.cn/flaw/show/CNVD-2023-55377

https://www.cnvd.org.cn/flaw/show/CNVD-2023-55378

https://www.cnvd.org.cn/flaw/show/CNVD-2023-55380

https://www.cnvd.org.cn/flaw/show/CNVD-2023-55381

https://www.cnvd.org.cn/flaw/show/CNVD-2023-55382

5、WordPress 插件 Tags Cloud Manager 跨站脚本漏洞

WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，WordPress 插件 Tags Cloud Manager 被披露存在跨站脚本漏洞。漏洞是由于用户提供的输入验证不当造成的。攻击者可利用该漏洞窃取受害者基于 cookie 的身份验证凭据。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-2023-55362

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：https://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-2023-55031	Adobe Acrobat Reader 数字错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb23-24.html
CNVD-2023-55039	Mattermost 代码问题漏洞（CNVD-2023-55039）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://mattermost.com/security-updates/
CNVD-2023-55352	Mozilla Thunderbird 信任管理问题漏洞（CNVD-2023-55352）	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.thunderbird.net/zh-CN/features/
CNVD-2023-55367	Google Android 权限提升漏洞（CNVD-2023-55367）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2023-04-01
CNVD-2023-55372	Google Android 代码执行漏洞（CNVD-2023-55372）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2023-04-01
CNVD-2023-55390	Schneider Electric EcoStruxure Foxboro DCS 缓冲区溢出	高	厂商已发布了漏洞修复程序，请及时关注更新：

	漏洞		https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-164-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-164-04.pdf
CNVD-2023-55713	Siemens RUGGEDCOM ROX 跨站请求伪造漏洞	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://cert-portal.siemens.com/productcert/html/ssa-146325.html
CNVD-2023-55719	Manjaro Linux Pamac 本地提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gitlab.manjaro.org/applications/libpamac/-/commit/889aa1d74ad305bb28178396dcc16e5b5381ade6
CNVD-2023-55718	Smartbi 逻辑漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.smartbi.com.cn/
CNVD-2023-56239	Adobe Coldfusion 访问控制绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://coldfusion.adobe.com/

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，Mozilla、Apache、Google 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，提升权限，在系统上执行任意代码，导致拒绝服务等。另外，WordPress 插件 Tags Cloud Manager 被披露存在跨站脚本漏洞。攻击者可利用该漏洞窃取受害者基于 cookie 的身份验证凭据。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、 Milesight UR32L firewall_handler_set 函数缓冲区溢出漏洞（CNVD-2023-55360）

验证描述

Milesight UR32L 是中国星纵物联（Milesight）公司的一个 4G 工业路由器。

Milesight UR32L firewall_handler_set 函数存在缓冲区溢出漏洞，该漏洞是由于 firewall_handler_set 函数的边界检查不正确造成的。经过身份验证的远程攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致应用程序崩溃。

验证信息

POC 链接：https://talosintelligence.com/vulnerability_reports/TALOS-2023-1716

参考链接：https://nvd.nist.gov/vuln/detail/CVE-2023-25085

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. Citrix 修复了 Ubuntu 安全访问客户端中的一个安全缺陷

Citrix 解决了一个安全漏洞，跟踪为 CVE-2023-24492（CVSS 分数为 9.6），影响 Ubuntu 的安全访问客户端，可利用该客户端实现远程代码执行。

参考链接：https://securityaffairs.com/148405/security/citrix-critical-flaw-secure-access-client-for-ubuntu.html

2. 苹果在修复浏览问题后重新发布零日补丁

Apple 使用 RSR 补丁来解决影响 iPhone、iPad 和 Mac 设备的安全问题，并快速修补主要操作系统版本之间的攻击中主动利用的漏洞。

参考链接：https://www.bleepingcomputer.com/news/apple/apple-re-releases-zero-day-patch-after-fixing-browsing-issue/#google_vignette

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