国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 08 月 14 日-2023 年 08 月 20 日 **2023 年第 33 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 398 个，其中高危漏洞 170 个、中危漏洞 206 个、低危漏洞 22 个。漏洞平均分值为 6.48。本周收录的漏洞中，涉及 0day 漏洞 308 个（占 77%），其中互联网上出现“MotoCMS SQL 注入漏洞、Total CMS 文件上传漏洞”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 22602 个，与上周（6410 个）环比增加 2.53 倍。

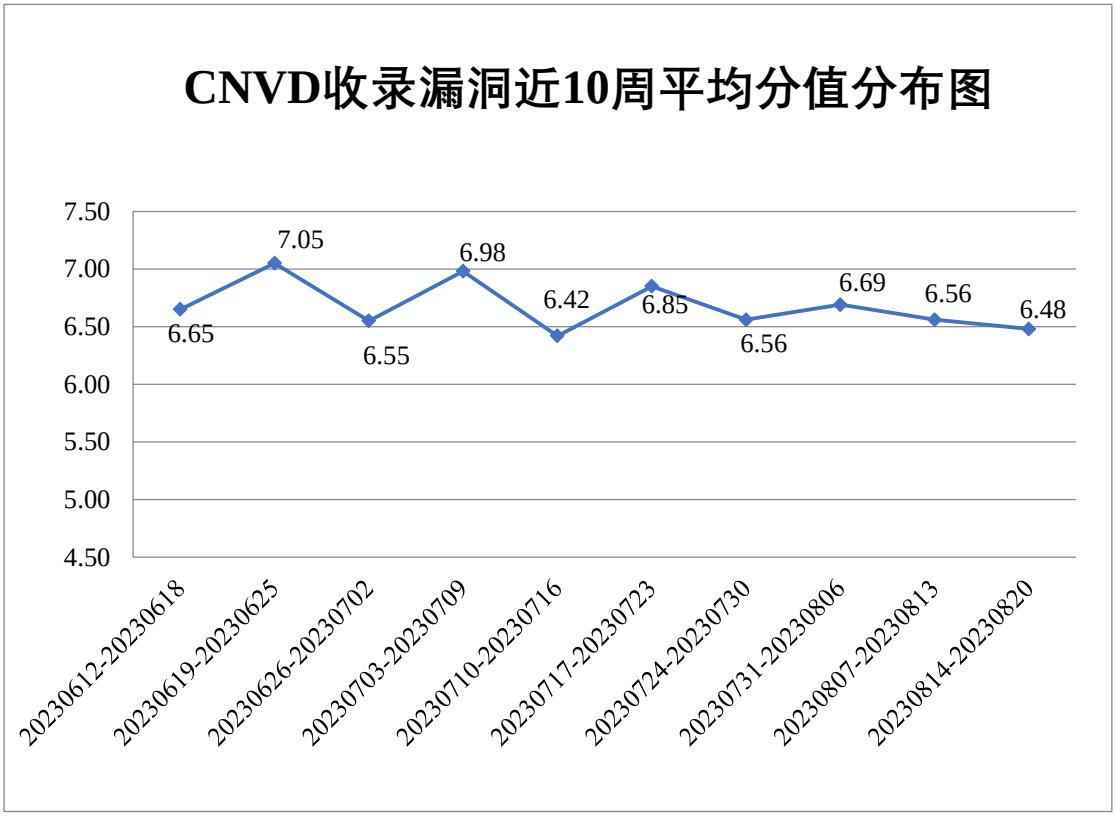

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 起，向基础电信企业通报漏洞事件 1 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 481 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 74 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 17 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：

重庆中联信息产业有限责任公司、中替车助（杭州）科技有限公司、中慈网络科技有限公司、正方软件股份有限公司、长春金阳高科技有限责任公司、渔翁信息技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、徐工集团工程机械股份有限公司、兄弟（中国）商业有限公司、星软集团有限公司、夏普商贸（中国）有限公司、西安三才科技实业有限公司、武汉达梦数据库有限公司、同望科技股份有限公司、通州区华丽软件工作室、天星数科科技有限公司、天维尔信息科技有限公司、天津天堰科技股份有限公司、泰尔茂医疗产品（上海）有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、四川易泊时捷智能科技有限公司、四川龙一医药有限公司、深圳左邻永佳科技有限公司、深圳中科鑫智科技有限公司、深圳智慧光迅信息技术有限公司、深圳市英威腾电气股份有限公司、深圳市网心科技有限公司、深圳市明源云科技有限公司、深圳市科脉技术股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市宏电技术股份有限公司、深圳市必联电子有限公司、深圳极数充物联技术有限公司、深圳古瑞瓦特新能源股份有限公司、上海卓卓网络科技有限公司、上海商派网络科技有限公司、上海米健信息急救有限公司、上海泛微网络科技股份有限公司、熵基科技股份有限公司、山东手麦智能科技有限公司、厦门四信通信科技有限公司、奇安信网神信息技术（北京）股份有限公司、奇安信科技集团股份有限公司、普联技术有限公司、蓝网科技股份有限公司、敬业钢铁有限公司、京瓷集团、金惠家科技有限公司、金蝶软件（中国）有限公司、捷安泊智慧停车管理有限公司、江苏卓易信息科技股份有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、汇思软件（上海）有限公司广州分公司、淮南市银泰软件科技有限公司、湖南省众达数蔚信息技术有限公司、湖南玛丽莱珠宝集团有限公司、洪湖尔创网联信息技术有限公司、河南省脱颖实业有限公司、河南惠旭利科技有限公司、合肥贰道网络科技有限公司、杭州映云科技有限公司、杭州伊柯夫科技有限公司、杭州千格源科技有限公司、杭州美软信息技术有限公司、杭州九言科技股份有限公司、杭州翰臣科技有限公司、桂林崇胜网络科技有限公司、广州图创计算机软件开发有限公司、广州思迈特软件有限公司、广州睿狐科技有限公司、广东卓锐软件有限公司、富士施乐（中国）有限公司、富士胶片商业创新（中国）有限

公司、福州银达云创信息科技有限公司、福建金网际软件科技有限公司、福建博思软件股份有限公司、大连不老一族网络科技有限公司、成都康特电子科技股份有限公司、成都飞鱼星科技股份有限公司、成都德芯数字科技股份有限公司、北京卓正志远软件有限公司、北京中创视讯科技有限公司、北京星网锐捷网络技术有限公司、北京文华在线教育科技股份有限公司、北京文安智能技术股份有限公司、北京网康科技有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京时代亿信科技股份有限公司、北京神州视翰科技有限公司、北京荣宝斋科技有限公司、北京猎鹰安全科技有限公司、北京旷视科技有限公司、北京久其软件股份有限公司、北京金和网络股份有限公司、北京环球国广媒体科技有限公司、北京宏景世纪软件股份有限公司、北京布瑞克农信科技集团有限责任公司、北京百卓网络技术有限公司、北京澳际教育咨询有限公司、奥泰尔科技有限公司、傲拓科技股份有限公司、安科瑞电气股份有限公司、安徽共生物流科技有限公司、WDJA、WAVLINK、semcms、Fujifilm 和 BEESCMS。

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、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司等单位报送公开收集的漏洞数量较多。联想集团、河南东方云盾信息技术有限公司、快页信息技术有限公司、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、安徽锋刃信息科技有限公司、河南灵创电子科技有限公司、重庆电信系统集成有限公司、赛尔网络有限公司、智网安云（武汉）信息技术有限公司、杭州弘沿科技有限公司、亚信科技（成都）有限公司、合肥梆梆信息科技有限公司、信息产业信息安全测评中心、北京六方云信息技术有限公司、浙江东安检测技术有限公司、北京安帝科技有限公司、北京航空航天大学、神州灵云（北京）科技有限公司、北京水木羽林科技有限公司、深圳市魔方安全科技有限公司、中华人民共和国广东海事局、山东正中信息技术股份有限公司、中国烟草总公司湖北省公司、海南神州希望网络有限公司、宁夏凯信特信息科技有限公司、南方电网数字电网集团信息通信科技有限公司及其他个人白帽子向 CNVD 提交了 22602 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）、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 21444 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）	20000	20000
新华三技术有限公司	738	0

三六零数字安全科技集团有限公司	728	728
上海交大	716	716
深信服科技股份有限公司	507	0
北京神州绿盟科技有限公司	448	0
北京天融信网络安全技术有限公司	238	0
远江盛邦（北京）网络安全科技股份有限公司	116	116
天津市国瑞数码安全系统股份有限公司	110	0
阿里云计算有限公司	101	0
北京启明星辰信息安全技术有限公司	82	11
安天科技集团股份有限公司	70	0
杭州安恒信息技术股份有限公司	23	23
杭州迪普科技股份有限公司	19	0
联想集团	83	83
河南东方云盾信息技术有限公司	48	48
快页信息技术有限公司	36	36
北京山石网科信息技术有限公司	13	13
河南信安世纪科技有限公司	12	12
安徽锋刃信息科技有限公司	10	10
河南灵创电子科技有	9	9

限公司		
重庆电信系统集成有限公司	5	5
赛尔网络有限公司	4	4
智网安云（武汉）信息技术有限公司	4	4
杭州弘沿科技有限公司	4	4
亚信科技（成都）有限公司	4	4
合肥梆梆信息科技有限公司	3	3
信息产业信息安全测评中心	3	3
北京六方云信息技术有限公司	2	2
浙江东安检测技术有限公司	1	1
北京安帝科技有限公司	1	1
北京航空航天大学	1	1
神州灵云（北京）科技有限公司	1	1
北京水木羽林科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
中华人民共和国广东海事局	1	1
山东正中信息技术股份有限公司	1	1
中国烟草总公司湖北省公司	1	1
海南神州希望网络有限公司	1	1

宁夏凯信特信息科技有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
CNCERT 广西分中心	10	10
个人	746	746
报送总计	24904	22602

本周漏洞按类型和厂商统计

本周，CNVD 收录了 398 个漏洞。WEB 应用 202 个，应用程序 106 个，网络设备（交换机、路由器等网络端设备）57 个，操作系统 15 个，智能设备（物联网终端设备）13 个，安全产品 5 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	202
应用程序	106
网络设备（交换机、路由器等网络端设备）	57
操作系统	15
智能设备（物联网终端设备）	13
安全产品	5

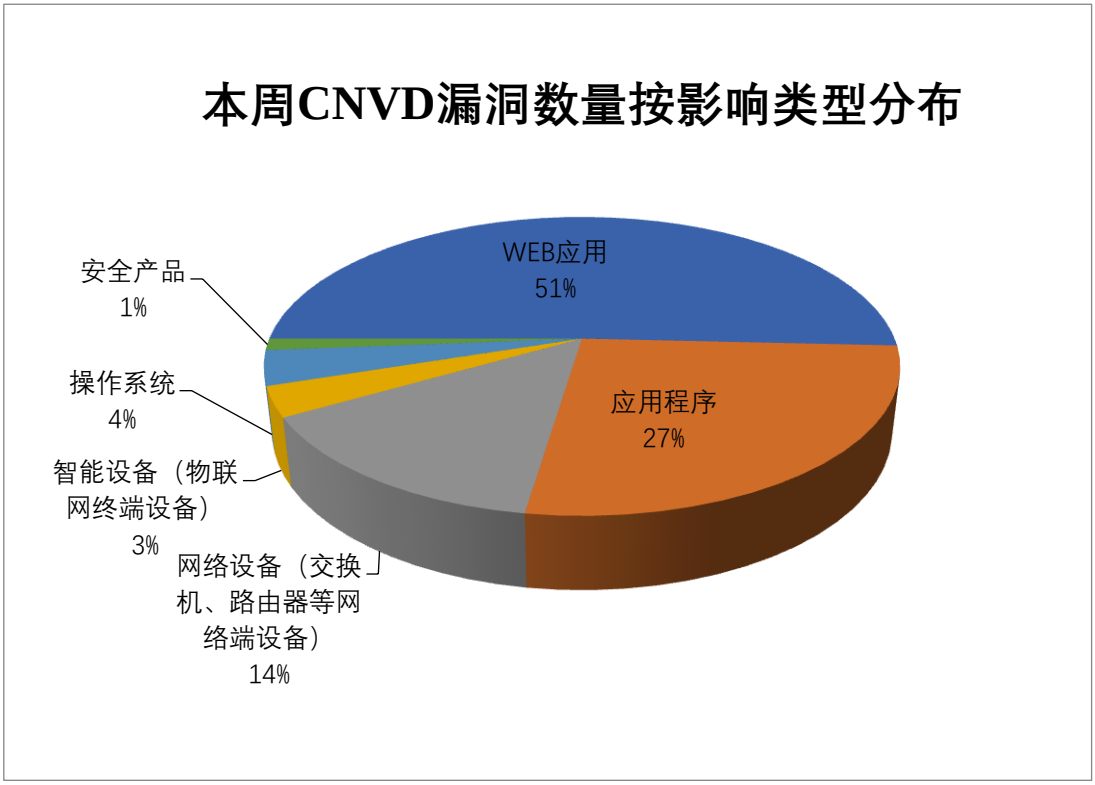

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、Linux 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	23	5%
2	Adobe	12	3%
3	Linux	10	3%
4	WordPress	10	3%
5	北京百卓网络技术有限公司	10	3%
6	Cisco	9	2%
7	新华三技术有限公司	7	2%
8	SEMCMS	7	2%
9	ASUS	6	1%
10	其他	304	76%

本周行业漏洞收录情况

本周，CNVD 收录了 42 个电信行业漏洞，44 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“Tenda 4G300 缓冲区溢出漏洞、TP-LINK Archer AX 21 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/

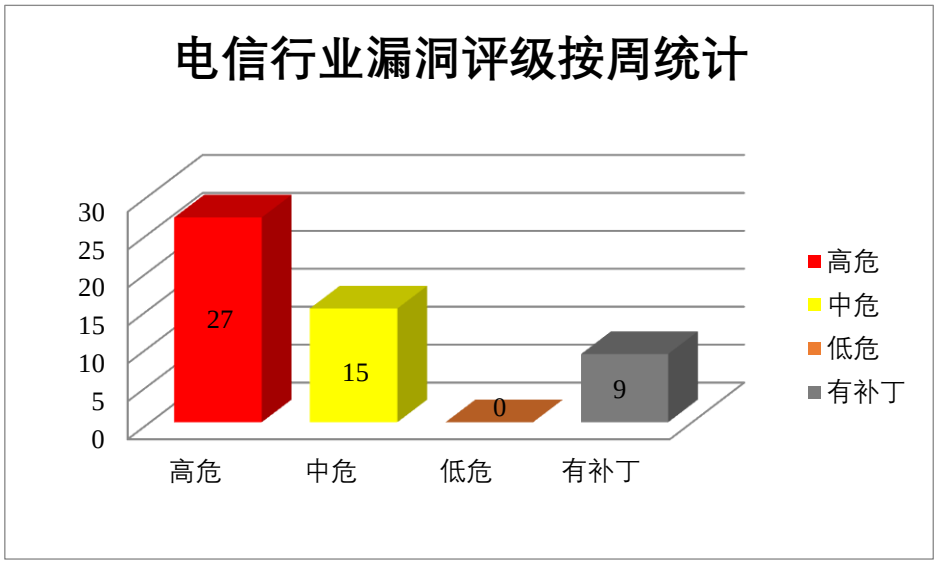

图 3 电信行业漏洞统计

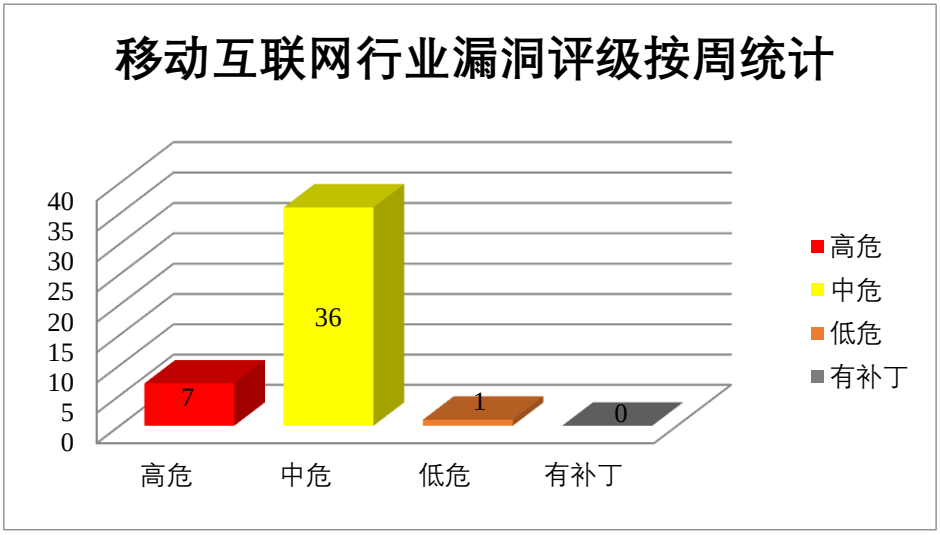

图 4 移动互联网行业漏洞统计

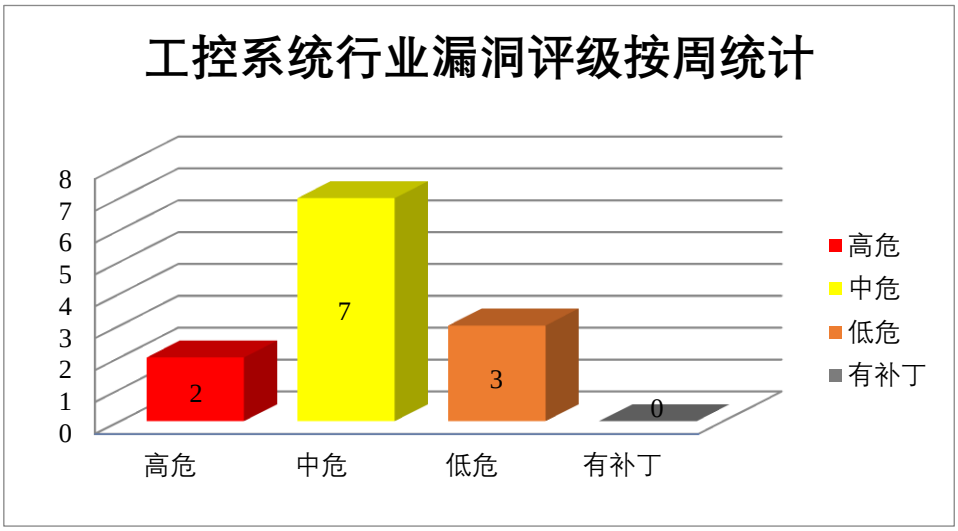

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2023-63463、CNVD-2023-63464、CNVD-2023-63465、CNVD-2023-63467、CNVD-2023-63468、CNVD-2023-63469、CNVD-2023-63470、CNVD-2023-63471）。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-2023-63463

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63464

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63465

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63467

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63468

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63469

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63470

https://www.cnvd.org.cn/flaw/show/CNVD-2023-63471

2、 Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。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越界读取，系统崩溃或提升其在系

统上的权限等。

CNVD 收录的相关漏洞包括：Linux kernel 内存错误引用漏洞（CNVD-2023-62923）、Linux kernel 拒绝服务漏洞（CNVD-2023-62922）、Linux kernel 缓冲区溢出漏洞（CNVD-2023-62927）、Linux kernel 越界读取漏洞（CNVD-2023-62926）、Linux kernel vcs_read 内存错误引用漏洞、Linux kernel 输入验证错误漏洞（CNVD-2023-62931）、Linux kernel fbcon.c 文件越界读取漏洞、Linux kernel smb2pdu.c 文件越界读取漏洞（CNVD-2023-62929）。其中，“Linux kernel 拒绝服务漏洞（CNVD-2023-62922）、Linux kernel 输入验证错误漏洞（CNVD-2023-62931）、Linux kernel smb2pdu.c 文件越界读取漏洞（CNVD-2023-62929）”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-2023-62923
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62922
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62927
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62926
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62925
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62931
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62930
https://www.cnvd.org.cn/flaw/show/CNVD-2023-62929

3、Cisco 产品安全漏洞

Cisco Webex Meetings 是美国思科（Cisco）公司的一套视频会议解决方案。Cisco SD-WAN vManage 是美国思科（Cisco）公司的一个高度可定制的仪表板。可简化和自动化 Cisco SD-WAN 的部署、配置、管理和操作。Cisco AsyncOS 是美国思科（Cisco）公司的产品。Cisco AsyncOS 是一款应用于思科设备的操作系统。Cisco DNA Center 是美国思科（Cisco）公司的一个网络管理和命令中心服务。Cisco Secure Workload 是美国思科（Cisco）公司的一种允许用户在其应用程序工作负载上安装软件代理的软件。Cisco StarOS 是美国思科（Cisco）公司的一套虚拟化操作系统。Cisco Smart Software Manager On-Prem（SSM On-Prem）是美国思科（Cisco）公司的一款用于 Cisco 产品许可证管理的组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，获得读取权限或有限的写入权限，以根用户身份从受限容器中读取信息、枚举用户信息或在受限容器中执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco Webex Meetings 跨站脚本漏洞（CNVD-2023-62934）、Cisco SD-WAN vManage 输入验证错误漏洞（CNVD-2023-62933）、Cisco AsyncOS 输入验证错误漏洞、Cisco DNA Center 授权问题漏洞、Cisco Secure Workload OpenAPI 特权提升漏洞、Cisco Webex Meetings 跨站请求伪造漏洞、Cisco StarOS 输

入验证错误漏洞、Cisco Smart Software Manager On-Prem SQL 注入漏洞。其中，“Cisco SD-WAN vManage 输入验证错误漏洞（CNVD-2023-62933）、Cisco StarOS 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-2023-62934

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62933

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62932

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62937

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62936

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62935

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62940

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62939

4、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，攻击者可利用漏洞导致敏感内存泄露，通过绕过 API 黑名单功能在当前用户的上下文中导致任意代码执行等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 越界读取漏洞（CNVD-2023-62945、CNVD-2023-62948、CNVD-2023-62946、CNVD-2023-62951、CNVD-2023-62949、CNVD-2023-62953）、Adobe Acrobat Reader 访问控制错误漏洞（CNVD-2023-62944）、Adobe Acrobat Reader 越界写入漏洞（CNVD-2023-62947）。其中“Adobe Acrobat Reader 访问控制错误漏洞（CNVD-2023-62944）、Adobe Acrobat Reader 越界写入漏洞（CNVD-2023-62947）、Adobe Acrobat Reader 越界读取漏洞（CNVD-2023-62951）”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-2023-62945

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62944

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62948

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62947

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62946

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62951

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62949

https://www.cnvd.org.cn/flaw/show/CNVD-2023-62953

5、ASUS RT-AX88U ej.c 缓冲区溢出漏洞

ASUS RT-AX88U 是中国华硕（ASUS）公司的一个无线路由器。本周，ASUS RT-AX88U 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞向设备发送特制请求，导致 h

ttpd 二进制文件在 ej.c 的 do_json_decode()函数中崩溃，从而导致 DoS。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-2023-63439

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-2023-62943	Adobe Acrobat Reader 未初始化指针访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb23-30.html
CNVD-2023-62950	Adobe Acrobat Reader 未初始化指针访问漏洞（CNVD-2023-62950）	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/apsb23-30.html
CNVD-2023-62954	ZKTeco BioTime 密码重置漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://zkteco.com
CNVD-2023-62956	SEMCMS 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.sem-cms.com/xiazai.html
CNVD-2023-63197	Discourse 身份验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/discourse/discourse-patreon/security/advisories/GHSA-fvj9-f67v-qpr4
CNVD-2023-63199	Synology Presto File Server 路径遍历漏洞	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.synology.cn/zh-cn/security/advisory/Synology_SA_22_19
CNVD-2023-63436	ASUS RT-AC66U 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.asus.com/us/networking-iot-servers/wifi-routers/asus-wifi-routers/rt-ac66u-b1/
CNVD-2023-63443	ASUS RT-AX82U 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.asus.com/us/networking-iot-servers/wifi-routers/asus-gaming-routers/rt-ax82u/
CNVD-2023	Google Chrome 安全绕过漏	高	厂商已发布了漏洞修复程序，请及

-63444	洞（CNVD-2023-63444）		时关注更新：https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_29.html
CNVD-2023-63466	Google Chrome 缓冲区溢出漏洞（CNVD-2023-63466）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码或导致应用程序崩溃。此外，Linux、Cisco、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致越界读取，系统崩溃或提升其在系统上的权限，以根用户身份从受限容器中读取信息、枚举用户信息或在受限容器中执行任意命令等。另外，ASUS RT-AX88U 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞向设备发送特制请求，导致 httpd 二进制文件在 ej.c 的 do_json_decode()函数中崩溃，从而导致 DoS。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、MotoCMS SQL 注入漏洞

验证描述

MotoCMS 是 MotoCMS 公司的一个简单的网站构建器。

MotoCMS v3.4.3 版本存在 SQL 注入漏洞，该漏洞源于应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞通过搜索功能的 keyword 参数来获取权限。

验证信息

POC 链接：https://www.exploit-db.com/exploits/51504

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-62941

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. 谷歌浏览器的新功能提醒用户自动删除恶意扩展程序

谷歌宣布计划在其即将推出的 Chrome 网络浏览器版本中增加一项新功能，以便在用户安装的扩展程序已从 Chrome 网上应用店中删除时提醒用户。

参考链接：https://thehackernews.com/2023/08/google-chromes-new-feature-alerts-users.html

2. Microsoft PowerShell Gallery 容易受到供应链攻击

Microsoft 的 PowerShell Gallery 代码存储库中宽松的软件包命名策略允许威胁参与者执行域名仿冒攻击，欺骗流行的软件包，并可能为大规模供应链攻击奠定基础。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-powershell-gallery-vulnerable-to-spoofing-supply-chain-attacks/

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