国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 02 月 27 日-2023 年 03 月 05 日 **2023 年第 9 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 234 个，其中高危漏洞 154 个、中危漏洞 72 个、低危漏洞 8 个。漏洞平均分值为 6.93。本周收录的漏洞中，涉及 0day 漏洞 163 个（占 70%），其中互联网上出现“SWFTools getGifDelayTime 函数缓冲区溢出漏洞、Bento4 AP4_HdlrAtom::AP4_HdlrAtom 函数拒绝服务漏洞”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 8956 个，与上周（10131 个）环比减少 12%。

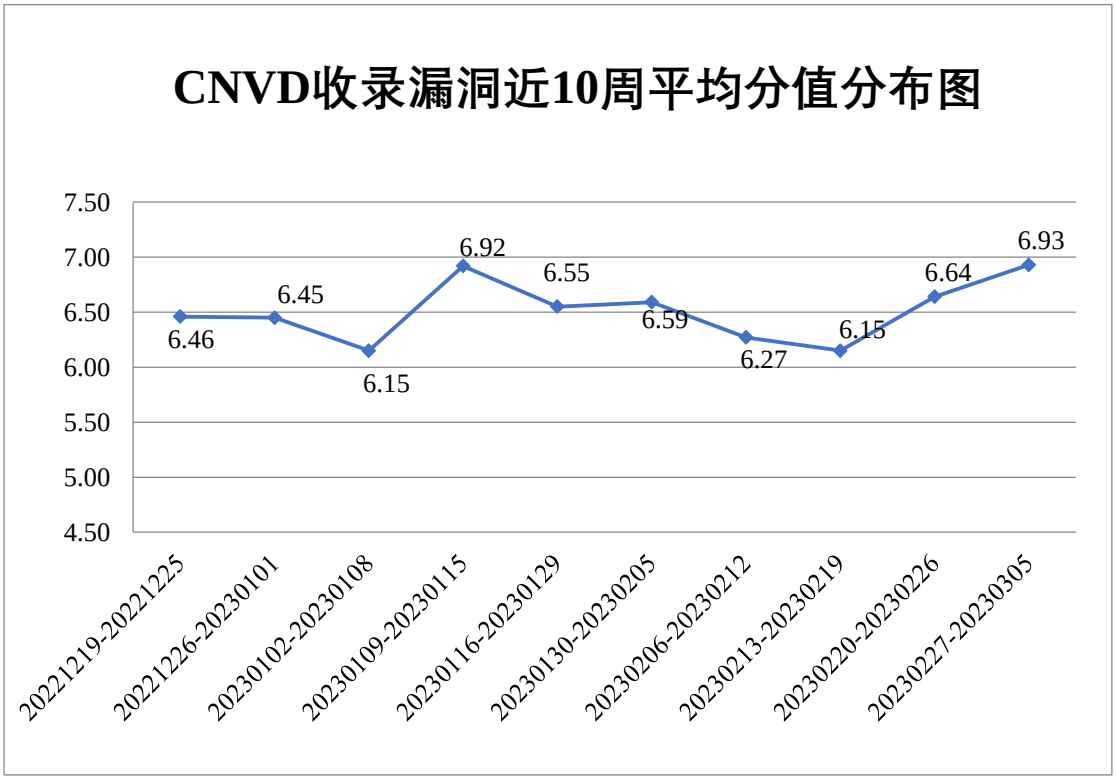

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电信企业通报漏洞事件 124 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 257 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 115 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：

海市泰德企业有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、中教智网（北京）信息技术有限公司、正方软件股份有限公司、浙江浙大中控信息技术有限公司、浙江宇视科技有限公司、浙江甲骨文超级码科技股份有限公司、长沙微康信息科技有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、武汉达梦数据库股份有限公司、同方知网数字出版技术股份有限公司、天维尔信息科技股份有限公司、苏州科达科技股份有限公司、四川鱼尾巴科技有限公司、四川永祥股份有限公司、沈阳明致软件有限公司、神州数码控股有限公司、深圳维盟科技股份有限公司、深圳市置辰海信科技有限公司、深圳市同为数码科技股份有限公司、深圳市锐明技术股份有限公司、深圳市明源云科技有限公司、深圳市科荣软件股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市宏电技术股份有限公司、深圳市东宝信息技术有限公司、深圳市必联电子有限公司、申瓯通信设备有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海英立视数字科技有限公司、上海联影医疗科技股份有限公司、上海酆泽信息技术有限公司、上海博达数据通信有限公司、熵基科技股份有限公司、商派软件有限公司、山西供销农芯乐电子商务有限公司、山东金榜苑文化传媒有限责任公司、厦门四信通信科技有限公司、瑞斯康达科技发展股份有限公司、任子行网络技术股份有限公司、千城智联（上海）网络科技有限公司、普联技术有限公司、南昌腾速科技有限公司、南昌北创科技发展有限公司、漯河市大有前途网络科技有限公司、朗坤智慧科技股份有限公司、蓝凌软件股份有限公司、金蝶软件（中国）有限公司、吉翁电子（深圳）有限公司、华信数安（深圳）技术有限公司、华录智达科技股份有限公司、湖南强智科技发展有限公司、湖南创星科技股份有限公司、弘扬软件股份有限公司、杭州逐一科技有限公司、杭州中沛电子有限公司、杭州雄伟科技开发股份有限公司、杭州迦智科技有限公司、杭州合泰软件有限公司、杭州当虹科技股份有限公司、国泰新点软件股份有限公司、国民技术股份有限公司、广州市丰华生物股份有限公司、广东天琴信息技术有限公司、福建福昕软件开发股份有限公司、东莞市通天星软件科技有限公司、东方网力科技股份有限公司、东北师大理想软件股份有限公司、当代教育科技集团有限公司、大唐电信科技股份有限公司、成都行行行科技有限公司、成都零起飞科技有限公司、畅捷通信息技术股份有限公司、北京中知智

慧科技有限公司、北京中园搏望科技发展有限公司、北京中新天达科技有限公司、北京云中融信网络科技有限公司、北京云帆互联科技有限公司、北京亿赛通科技发展有限责任公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京信安世纪科技有限公司、北京通达志成科技有限公司、北京谋智火狐信息技术有限公司、北京九思协同软件有限公司、北京格胜科技有限公司、北京春笛网络信息技术服务有限公司和北京百度网讯科技有限公司。

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、北京启明星辰信息安全技术有限公司、新华三技术有限公司、安天科技集团股份有限公司、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。北京山石网科信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州默安科技有限公司、北京升鑫网络科技有限公司、快页信息技术有限公司、上海齐同信息科技有限公司、河南东方云盾信息技术有限公司、福建省海峡信息技术有限公司、杭州海康威视数字技术股份有限公司、湖南轻山信息技术有限公司、江西诚韬科技有限公司、星云博创科技有限公司、浙江安腾信息技术有限公司、北京网御星云信息技术有限公司、北京君云天下科技有限公司、内蒙古洞明科技有限公司、安徽锋刃信息科技有限公司、宁夏凯信特信息科技有限公司、赛尔网络有限公司、苏州棱镜七彩信息科技有限公司、山东鼎夏智能科技有限公司、重庆都会信息科技有限公司、博智安全科技股份有限公司、北京众安天下科技有限公司、上海谋乐网络科技有限公司、北京华顺信安信息技术有限公司、河南灵创电子科技有限公司、郑州埃文科技、玄蜂安全团队、江苏保旺达软件技术有限公司、山东新潮信息技术有限公司、河南天祺信息安全技术有限公司、广州安亿信软件科技有限公司、平安银河实验室、武汉非尼克斯软件技术有限公司、内蒙古信元网络安全技术股份有限公司、河北锐远网络科技有限公司、南方电网数字电网集团信息通信科技有限公司、北京云梦创网络科技有限公司、西安长盛信安信息技术有限公司、河南悦海数安科技有限公司、中通服创发科技有限责任公司、云南联创网安科技有限公司、合肥梆梆信息科技有限公司、华泰证券股份有限公司、重庆易阅科技有限公司及其他个人白帽子向 CNVD 提交了 8956 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）、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 5520 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）	1821	1821

斗象科技（漏洞盒子）	1779	1779
三六零数字安全科技集团有限公司	1050	1050
上海交大	870	870
深信服科技股份有限公司	521	0
北京启明星辰信息安全技术有限公司	443	6
新华三技术有限公司	397	0
安天科技集团股份有限公司	295	0
阿里云计算有限公司	256	17
北京天融信网络安全技术有限公司	160	11
天津市国瑞数码安全系统股份有限公司	118	0
恒安嘉新（北京）科技股份公司	70	0
北京数字观星科技有限公司	67	0
杭州安恒信息技术股份有限公司	61	23
中国电信集团系统集成有限责任公司	58	0
卫士通信息产业股份有限公司	37	0
杭州迪普科技股份有限公司	15	1
北京知道创宇信息技术有限公司	17	0
京东科技信息技术有限公司	8	1
南京众智维信息科技有限公司	6	6
远江盛邦（北京）网	3	3

络安全科技股份有限公司		
西安四叶草信息技术有限公司	2	2
北京长亭科技有限公司	2	2
深圳市腾讯计算机系统有限公司（玄武实验室）	2	2
北京信联数安科技有限公司	1	1
北京神州绿盟科技有限公司	1	1
北京山石网科信息技术有限公司	56	56
奇安星城网络安全运营服务（长沙）有限公司	52	52
杭州默安科技有限公司	52	52
北京升鑫网络科技有限公司	45	45
快页信息技术有限公司	34	34
上海齐同信息科技有限公司	34	34
河南东方云盾信息技术有限公司	25	25
福建省海峡信息技术有限公司	13	13
杭州海康威视数字技术股份有限公司	13	13
湖南轻山信息技术有限公司	11	11
江西诚韬科技有限公	9	9

司		
星云博创科技有限公司	8	8
浙江安腾信息技术有限公司	7	7
北京网御星云信息技术有限公司	7	7
北京君云天下科技有限公司	7	7
内蒙古洞明科技有限公司	6	6
安徽锋刃信息科技有限公司	5	5
宁夏凯信特信息科技有限公司	5	5
赛尔网络有限公司	4	4
苏州棱镜七彩信息科技有限公司	4	4
山东鼎夏智能科技有限公司	3	3
重庆都会信息科技有限公司	3	3
博智安全科技股份有限公司	3	3
北京众安天下科技有限公司	3	3
上海谋乐网络科技有限公司	3	3
北京华顺信安信息技术有限公司	2	1
河南灵创电子科技有限公司	2	2
郑州埃文科技	2	2
玄蜂安全团队	2	2
江苏保旺达软件技术	2	2

有限公司		
山东新潮信息技术有限公司	2	2
河南天祺信息安全技术有限公司	2	2
广州安亿信软件科技有限公司	2	2
平安银河实验室	1	1
武汉非尼克斯软件技术有限公司	1	1
内蒙古信元网络安全技术股份有限公司	1	1
河北镌远网络科技有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
北京云梦创网络科技有限公司	1	1
西安长盛信安信息技术有限公司	1	1
河南悦海数安科技有限公司	1	1
中通服创发科技有限责任公司	1	1
云南联创网安科技有限公司	1	1
合肥梆梆信息科技有限公司	1	1
华泰证券股份有限公司	1	1
重庆易阅科技有限公司	1	1
亚信科技（成都）有限公司	1	0

CNCERT 广西分中心	3	3
CNCERT 贵州分中心	1	1
个人	2916	2916
报送总计	11422	8956

本周漏洞按类型和厂商统计

本周，CNVD 收录了 234 个漏洞。WEB 应用 95 个，应用程序 59 个，网络设备（交换机、路由器等网络端设备）48 个，操作系统 26 个，安全产品 2 个，智能设备（物联网终端设备）2 个，数据库 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	95
应用程序	59
网络设备（交换机、路由器等网络端设备）	48
操作系统	26
安全产品	2
智能设备（物联网终端设备）	2
数据库	2

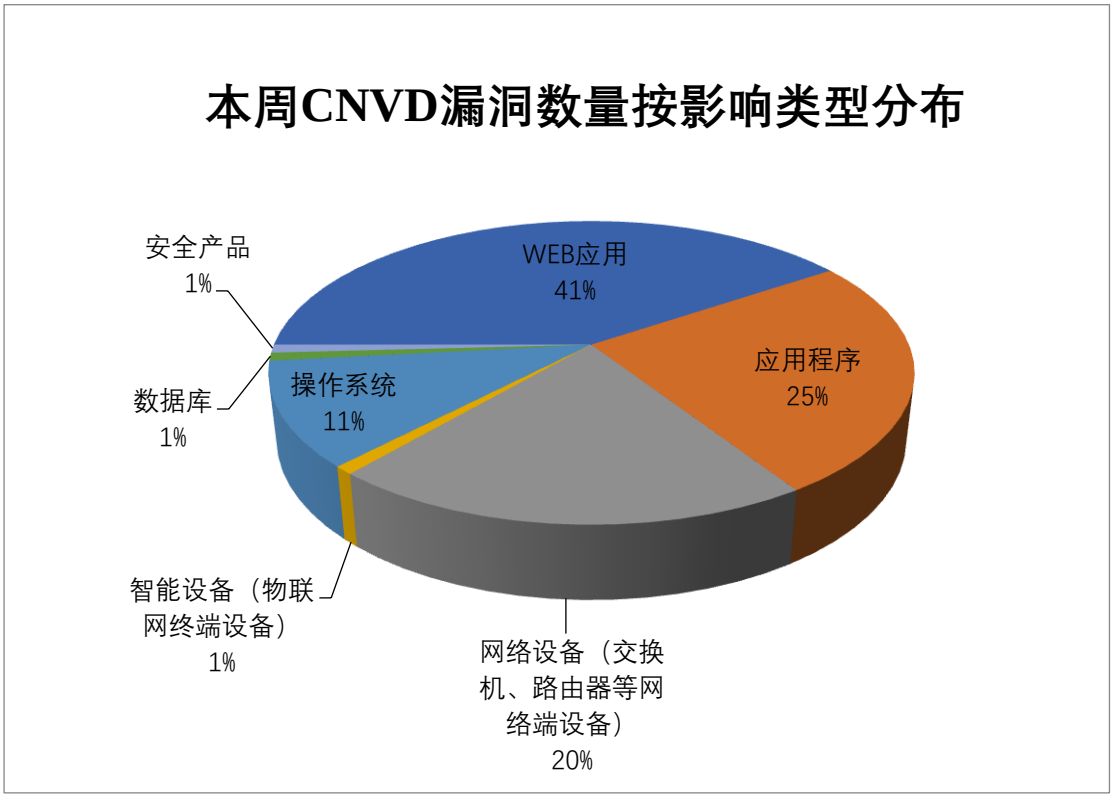

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 DELL、Adobe、Tenda 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	DELL	20	9%
2	Adobe	17	7%
3	Tenda	14	6%
4	深圳市和为顺网络技术有限公司	13	6%
5	Google	13	6%
6	SIEMENS	10	4%
7	Online Food Ordering System	8	3%
8	北京网康科技有限公司	7	3%
9	TOTOLINK	6	3%
10	其他	126	53%

本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，15 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，“Google Android 权限提升漏洞（CNVD-2023-14290）、Schneider Electric IGSS Data Server 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/

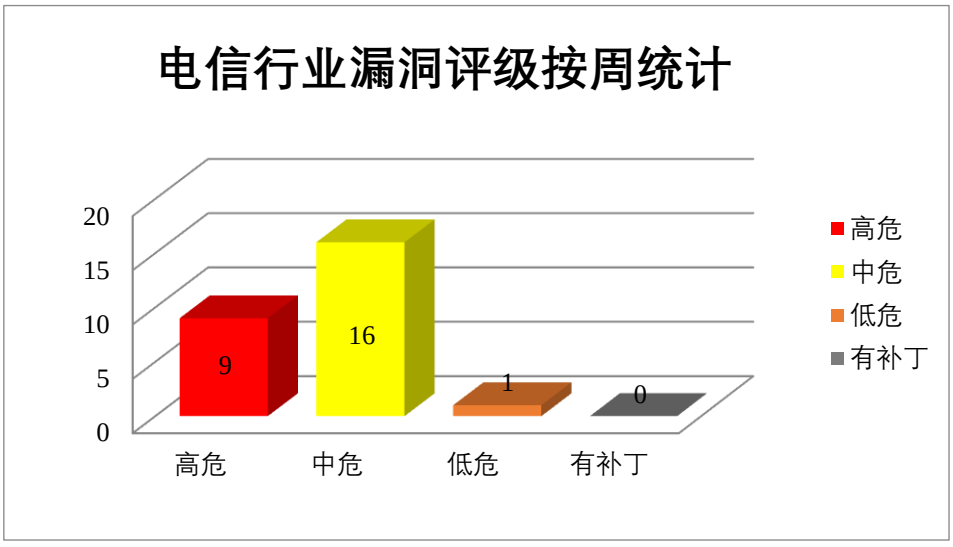

图 3 电信行业漏洞统计

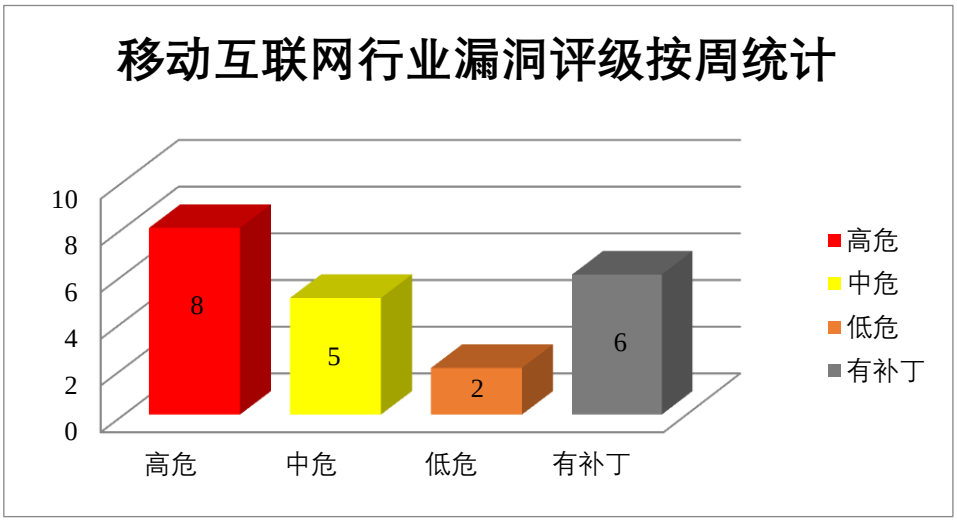

图 4 移动互联网行业漏洞统计

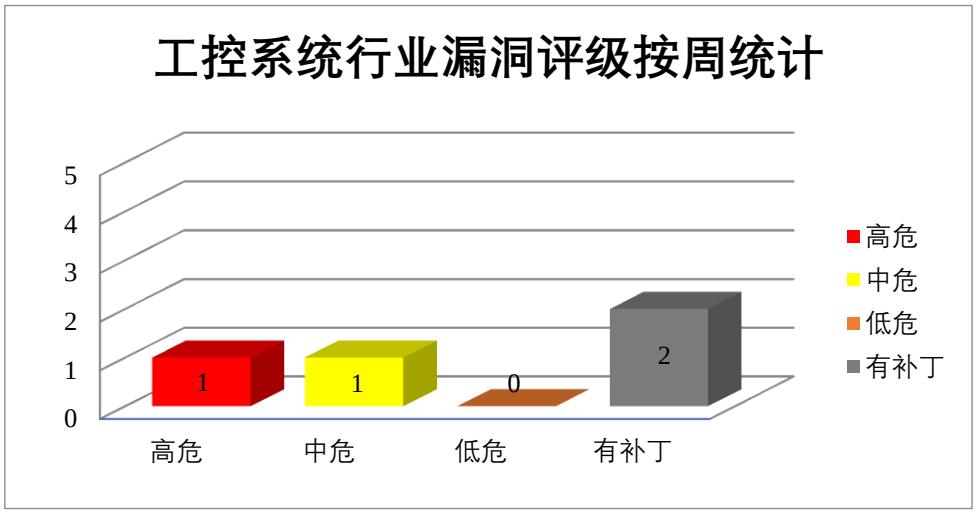

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens Tecnomatix Plant Simulation 是面向对象的、图形化的、集成的建模、仿真工具。Siemens Parasolid 是德国西门子（Siemens）公司的一个几何建模内核。Siemens Solid Edge 是德国西门子（Siemens）公司的一款三维 CAD 软件。该软件可用于零件设计、装配设计、钣金设计、焊接设计等行业。JT Open Toolkit 是为支持 JT 的软件开发人员提供的应用程序编程接口（API）。JT 是由西门子数字工业软件开发的公开发布的数据格式，广泛用于通信、可视化、数字模型和各种其他目的。Siemens Comos 是德国西门子（Siemens）公司的一个工厂工程软件解决方案。用于过程工业。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者导致拒绝服务。

CNVD 收录的相关漏洞包括：Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-13089、CNVD-2023-13088、CNVD-2023-13087、CNVD-2023-13090、CNVD-2023-13095）、Siemens Parasolid 和 Solid Edge SE2022 越界读取漏洞、Siemens JT Open 和 JT Utilitiesh 内存破坏漏洞、Siemens Comos 缓冲区溢出漏洞。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-2023-13089

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13088

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13087

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13093

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13092

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13091

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13090

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13095

2、 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 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，攻击者可利用漏洞通过特制的 HTML 页面绕过内容安全策略，泄露跨域数据，提升权限等。

CNVD 收录的相关漏洞包括：Google Chrome V8 类型混淆漏洞（CNVD-2023-12021）、Google Android Kernel 权限提升漏洞（CNVD-2023-12019）、Google Chrome iframe Sandbox 代码问题漏洞、Google Chrome 安全特制问题漏洞、Google Chrome 信息泄露漏洞（CNVD-2023-12025、CNVD-2023-14253、CNVD-2023-14290、CNVD-2023-14291）。其中，除“Google Android Kernel 权限提升漏洞（CNVD-2023-12019）、Google Chrome 信息泄露漏洞（CNVD-2023-12025）”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-2023-12021

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12019

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12023

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12027

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12025

https://www.cnvd.org.cn/flaw/show/CNVD-2023-14253

https://www.cnvd.org.cn/flaw/show/CNVD-2023-14290

https://www.cnvd.org.cn/flaw/show/CNVD-2023-14291

3、Adobe 产品安全漏洞

Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。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用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe After Effects 输入验证错误漏洞、Adobe After Effects 越界写入漏洞（CNVD-2023-13729、CNVD-2023-13731）、Adobe Bridge 越界写入漏洞（CNVD-2023-13728、CNVD-2023-13734、CNVD-2023-14293）、Adobe Bridge 堆栈缓冲区溢出漏洞（CNVD-2023-13735）、Adobe Bridge 输入验证错误漏洞（CNVD-2023-14292）。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-2023-13730

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13729

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13728

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13731

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13735

https://www.cnvd.org.cn/flaw/show/CNVD-2023-13734

https://www.cnvd.org.cn/flaw/show/CNVD-2023-14292

https://www.cnvd.org.cn/flaw/show/CNVD-2023-14293

4、Dell 产品安全漏洞

Dell PowerScale OneFS 是美国戴尔（Dell）公司的提供横向扩展 NAS 的 PowerScale OneFS 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过多个受影响字段存储恶意 HTML 或 JavaScript 代码，获取敏感信息，导致系统崩溃等。

CNVD 收录的相关漏洞包括：Dell PowerScale OneFS 跨站脚本漏洞、Dell PowerScale OneFS 缓冲区溢出漏洞、Dell PowerScale OneFS 日志信息泄露漏洞（CNVD-2023-12626、CNVD-2023-12625、CNVD-2023-12630、CNVD-2023-12627）、Dell PowerScale OneFS 信任管理问题漏洞、Dell PowerScale OneFS 操作系统命令注入漏洞。其中，“Dell PowerScale OneFS 日志信息泄露漏洞（CNVD-2023-12626、CNVD-2023-12627）、Dell PowerScale OneFS 信任管理问题漏洞”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-2023-12615

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12614

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12626

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12625

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12623

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12627

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12631

https://www.cnvd.org.cn/flaw/show/CNVD-2023-12630

5、Tenda i9 formWifiMacFilterGet 函数缓冲区溢出漏洞

Tenda i9 是一款企业无线 AP 设备。本周，Tenda i9 formWifiMacFilterGet 函数存在缓冲区溢出漏洞。攻击者可利用该漏洞通过特制的字符串造成拒绝服务（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-2023-13082

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-2023-12024	Google Chrome 输入验证错误漏洞（CNVD-2023-12024）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html
CNVD-2023-12026	Google Chrome 缓冲区溢出漏洞（CNVD-2023-12026）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html
CNVD-2023-13080	Huawei HarmonyOS 授权问题漏洞（CNVD-2023-13080）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202211-0000001440896653
CNVD-2023-13094	Siemens SiPass integrated AC5102/ACC-G2 和 ACC-A 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-658793.pdf
CNVD-2023-13733	Adobe Animate 堆栈缓冲区溢出漏洞	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/animate/apsb23-15.html
CNVD-2023	Adobe FrameMaker 输入验证	高	厂商已发布了漏洞修复程序，请及

-14296	错误漏洞		时关注更新：https://helpx.adobe.com/security/products/framemaker/apsb23-06.html
CNVD-2023-14299	Tenda i9 formWifiMacFilterSet 函数缓冲区溢出漏洞	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.tenda.com.cn/
CNVD-2023-14300	Tenda i9 formwrlSSIDset 函数缓冲区溢出漏洞	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.tenda.com.cn/
CNVD-2023-14307	Schneider Electric IGSS Data Server 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-102-01
CNVD-2023-14304	Tenda i9 set_local_time 函数缓冲区溢出漏洞	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.tenda.com.cn/

小结：本周，Siemens 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者导致拒绝服务。此外，Google、Adobe、Dell 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTML 页面绕过内容安全策略，泄露跨域数据，提升权限，在当前用户的上下文中执行任意代码，导致系统崩溃等。另外，Tenda i9 formWifiMacFilterGet 函数被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过特制的字符串造成拒绝服务（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、SWFTools getGifDelayTime 函数缓冲区溢出漏洞

验证描述

SWFTools 是一组用于处理 Adobe Flash 文件（SWF 文件）的实用程序。

SWFTools commit 772e55a2 存在缓冲区溢出漏洞，该漏洞源于/home/bupt/Desktop/swftools/src/src/gif2swf.c 的 getGifDelayTime 函数在处理不受信任的输入时出现边界错误。攻击者可利用该漏洞导致程序崩溃。

验证信息

POC 链接：https://github.com/Cvjark/Poc/blob/main/swftools/gif2swf/CVE-2022-35088.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-13079

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. 火狐浏览器 Firefox 110.0.1 发布，修复了安全和崩溃问题

近期，Mozilla 发布了 Firefox 110.0.1 稳定版更新，本次更新重点修复了崩溃问题，并提高了浏览器的安全性。

参考链接：https://www.ithome.com/0/676/632.htm

2. 亚马逊、波音、宝马等软件供应商 Beeline 数据库遭攻击

当地时间 2 月 28 日消息，美国软件公司 Beeline 的数据库被攻击者发布在黑客论坛上，数据库内包含亚马逊、瑞士信贷、3M、波音、宝马、戴姆勒、摩根大通、麦当劳、蒙特利尔银行等 Beeline 客户的数据。

参考链接：https://www.freebuf.com/articles/database/359008.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