国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 03 月 06 日-2023 年 03 月 12 日 **2023 年第 10 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**高**。

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 241 个，其中高危漏洞 147 个、中危漏洞 81 个、低危漏洞 13 个。漏洞平均分值为 7.05。本周收录的漏洞中，涉及 0day 漏洞 165 个（占 68%），其中互联网上出现“Tenda AC23 堆栈溢出漏洞（CNVD-2023-15697）、yasm hash 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 28859 个，与上周（8956 个）环比增加 2.22 倍。

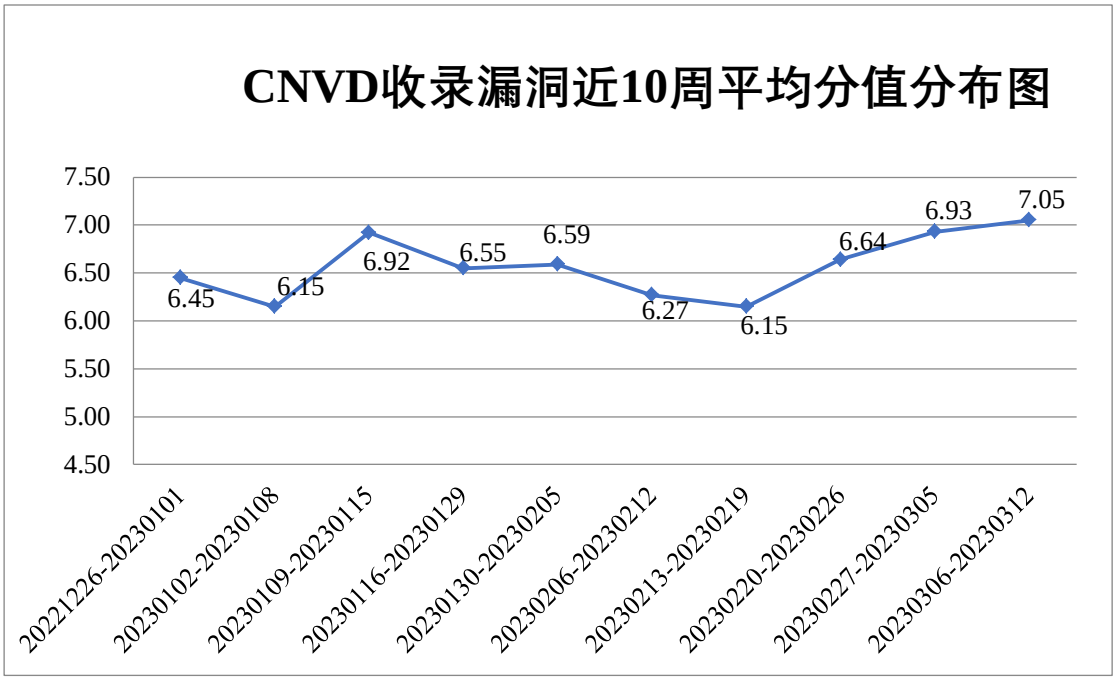

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电

信企业通报漏洞事件 92 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 505 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 210 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 112 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：

重庆森鑫炬科技有限公司、智秦数字出版集团有限公司、政和科技股份有限公司、浙江中控技术股份有限公司、漳州市芗城帝兴软件开发有限公司、用友网络科技股份有限公司、西安动力无限信息技术有限公司、腾讯安全应急响应中心、宿迁鑫潮信息技术有限公司、四川易泊时捷智能科技有限公司、深圳座联互动科技有限公司、深圳智慧光迅信息技术有限公司、深圳市科荣软件股份有限公司、深圳市和为顺网络技术有限公司、深圳勤杰软件有限公司、深圳古瑞瓦特科技能源有限责任公司、上海微盟企业发展有限公司、上海顺舟智能科技股份有限公司、上海上业信息科技股份有限公司、上海三高计算机中心股份有限公司、上海米健信息技术有限公司、上海酆泽信息技术有限公司、山脉科技股份有限公司、山东舒亨养老服务有限公司、山东山大华天软件有限公司、山东京帝软件有限公司、山东金钟科技集团股份有限公司、厦门天锐科技股份有限公司、厦门四信通信科技有限公司、青岛易软天创网络科技有限公司、青岛积成电子股份有限公司、普联技术有限公司、力合科技（湖南）股份有限公司、朗坤智慧科技股份有限公司、科大国创软件股份有限公司、开联通支付服务有限公司、敬业钢铁有限公司、金华迪加网络科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、慧星软件科技有限公司、惠尔丰信息系统有限公司、湖南创星科技股份有限公司、湖南畅乘科技有限公司、黑龙江立高科技股份有限公司、河北丰源智控科技股份有限公司、杭州三汇信息工程有限公司、杭州禾诺信息技术有限公司、杭州飞致云信息科技有限公司、哈尔滨伟成科技有限公司、广州同福信息科技有限公司、广州市丰华生物股份有限公司、广州酷狗计算机科技有限公司、广州丰益捷电子技术有限公司、广东鑫宝软件科技有限公司、馥鸿科技股份有限公司、法信公证云（厦门）科技有限公司、东北师大理想软件股份有限公司、成都卓越远扬信息技术有限公司、畅捷通信息技术股份有限公司、北京中科网威信息技术有限公司、北京易拓软件有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京万户软件技术有限公司、北京容大天成科技有限公司、北京派网软件有限公司#2、北京欧倍尔软件技术开发有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京东方智辰科技开发有限公司、北京北信源软件股份有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安徽省科迅教育装备有限公司、阿里巴巴集团安全应急响应中心、WAVLINK、NVIDIA 和 emlog。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、新华三技术有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、贵州泰若数字科技有限公司、博智安全科技股份有限公司、北京升鑫网络科技有限公司、上海齐同信息科技有限公司、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、河南东方云盾信息技术有限公司、北京安盟信息技术股份有限公司、快页信息技术有限公司、湖南轻山信息技术有限公司、浙江安腾信息技术有限公司、山东鼎夏智能科技有限公司、安徽锋刃信息科技有限公司、江西诚韬科技有限公司、山东网驰安全技术有限公司、苏州棱镜七彩信息科技有限公司、江苏金盾检测技术有限公司、重庆易阅科技有限公司、赛尔网络有限公司、北京威努特技术有限公司、中通服创发科技有限责任公司、宁夏凯信特信息科技有限公司、浙江大学控制科学与工程学院、国网浙江省电力有限公司、上海谋乐网络科技有限公司、北京安帝科技有限公司、山东云天安全技术有限公司、杭州海康威视数字技术股份有限公司、山东新潮信息技术有限公司、墨菲未来科技（北京）有限公司、郑州埃文科技、杭州默安科技有限公司、广州安亿信软件科技有限公司、成都安美勤信息技术股份有限公司、山东九域信息技术有限公司、华中科技大学、杭州美创科技有限公司、福建中信网安信息科技有限公司、江西和尔惠信息技术有限公司、河南灵创电子科技有限公司、北京众安天下科技有限公司、北京君云天下科技有限公司、中国电信股份有限公司上海研究院及其他个人白帽子向 CNVD 提交了 28859 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 25834 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）	20622	20622
斗象科技（漏洞盒子）	3005	3005
上海交大	1170	1170
三六零数字安全科技集团有限公司	1037	1037
北京启明星辰信息安全技术有限公司	370	0
深信服科技股份有限公司	351	0
新华三技术有限公司	285	0

北京神州绿盟科技有限公司	246	0
安天科技集团股份有限公司	234	0
阿里云计算有限公司	128	0
恒安嘉新（北京）科技股份公司	80	0
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	46	27
南京众智维信息科技有限公司	33	33
京东科技信息技术有限公司	15	0
杭州迪普科技股份有限公司	14	0
远江盛邦（北京）网络安全科技股份有限公司	7	7
北京天融信网络安全技术有限公司	5	5
中国电信股份有限公司网络安全产品运营中心	5	5
浙江大华技术股份有限公司	5	5
中国电信集团系统集成有限责任公司	3	3
北京安信天行科技有限公司	2	2
西安四叶草信息技术有限公司	1	1
北京华顺信安信息技术有限公司	609	0

贵州泰若数字科技有限公司	139	139
博智安全科技股份有限公司	121	121
北京升鑫网络科技有限公司	116	116
上海齐同信息科技有限公司	76	76
北京山石网科信息技术有限公司	54	54
奇安星城网络安全运营服务（长沙）有限公司	46	46
河南东方云盾信息技术有限公司	26	26
北京安盟信息技术股份有限公司	26	26
快页信息技术有限公司	18	18
湖南轻山信息技术有限公司	16	16
浙江安腾信息技术有限公司	15	15
山东鼎夏智能科技有限公司	14	14
安徽锋刃信息科技有限公司	9	9
江西诚韬科技有限公司	5	5
山东网驰安全技术有限公司	5	5
苏州棱镜七彩信息科技有限公司	4	4
江苏金盾检测技术有限公司	3	3

重庆易阅科技有限公司	3	3
赛尔网络有限公司	3	3
北京威努特技术有限公司	3	3
中通服创发科技有限责任公司	2	2
宁夏凯信特信息科技有限公司	2	2
浙江大学控制科学与工程学院	2	2
国网浙江省电力有限公司	2	2
上海谋乐网络科技有限公司	2	2
北京安帝科技有限公司	2	2
山东云天安全技术有限公司	2	2
杭州海康威视数字技术股份有限公司	2	2
山东新潮信息技术有限公司	2	2
墨菲未来科技（北京）有限公司	1	1
郑州埃文科技	1	1
杭州默安科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
山东九域信息技术有限公司	1	1
华中科技大学	1	1

杭州美创科技有限公司	1	1
福建中信网安信息科技有限公司	1	1
江西和尔惠信息技术有限公司	1	1
河南灵创电子科技有限公司	1	1
北京众安天下科技有限公司	1	1
北京君云天下科技有限公司	1	1
中国电信股份有限公司上海研究院	1	1
CNCERT 广西分中心	3	3
CNCERT 河北分中心	1	1
个人	2199	2199
报送总计	31269	28859

本周漏洞按类型和厂商统计

本周，CNVD 收录了 241 个漏洞。WEB 应用 94 个，应用程序 82 个，网络设备（交换机、路由器等网络端设备）58 个，操作系统 6 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	94
应用程序	82
网络设备（交换机、路由器等网络端设备）	58
操作系统	6
数据库	1

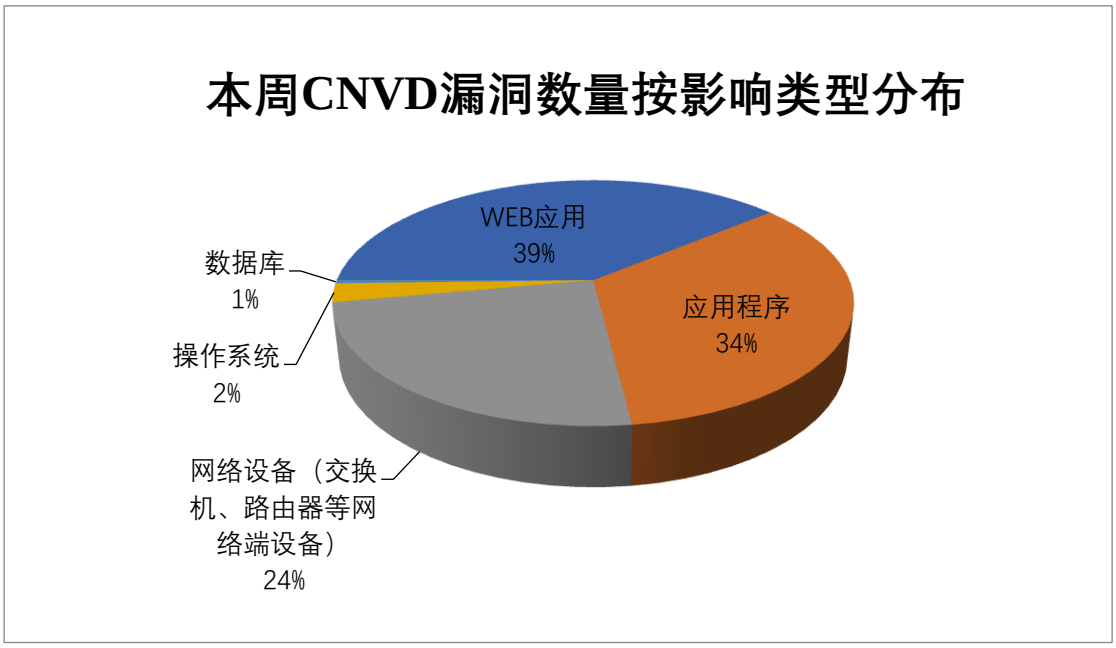

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 DELL、Google、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	14	6%
2	Google	12	5%
3	Tenda	11	5%
4	Adobe	10	4%
5	Mozilla	9	4%
6	Siemens	9	4%
7	yasm	8	3%
8	深圳市和为顺网络技术有限公司	7	3%
9	上海泛微网络科技股份有限公司	6	2%
10	其他	155	64%

本周行业漏洞收录情况

本周，CNVD 收录了 48 个电信行业漏洞，9 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Siretta QUARTZ-GOLD 缓冲区溢出漏洞（CNVD-2023-15941）、ZTE MF286R 命令注入漏洞”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/

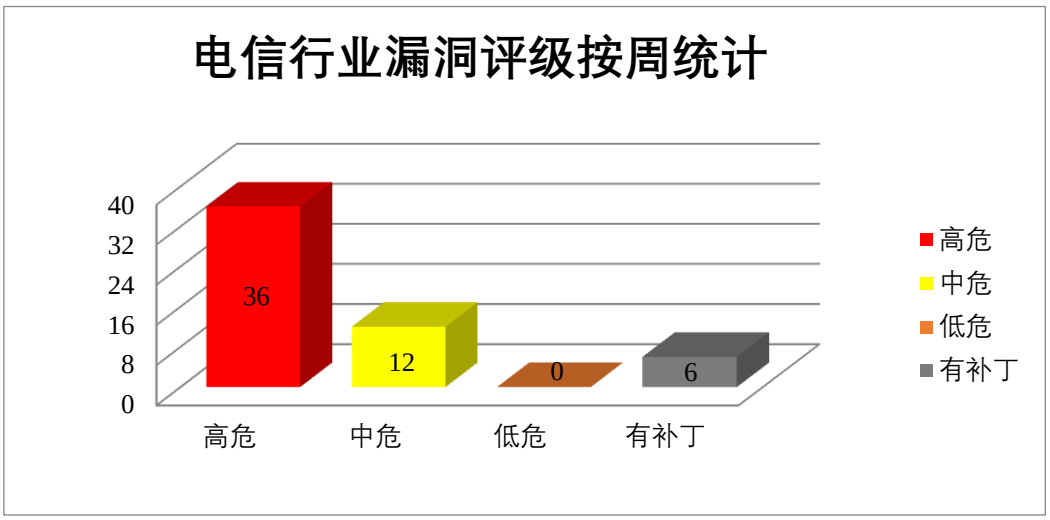

图 3 电信行业漏洞统计

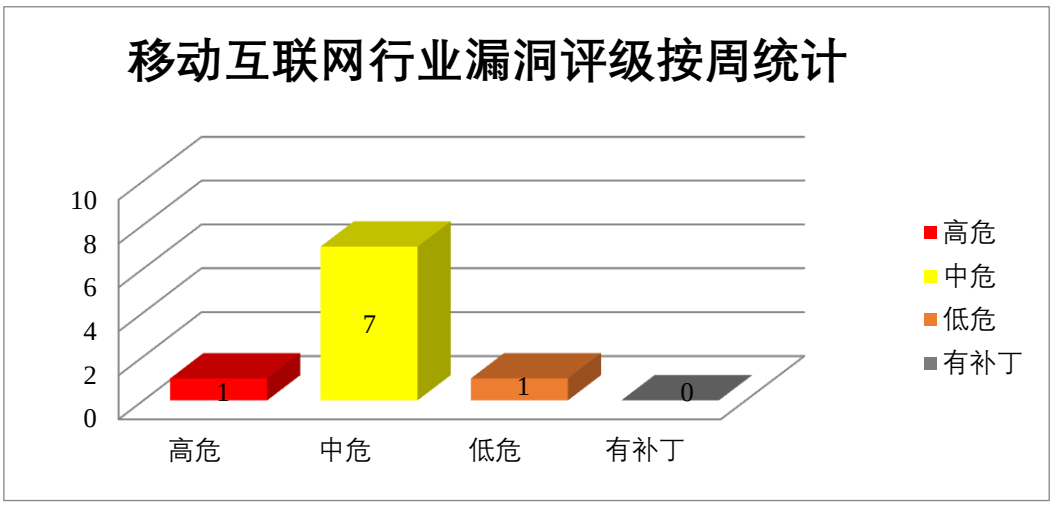

图 4 移动互联网行业漏洞统计

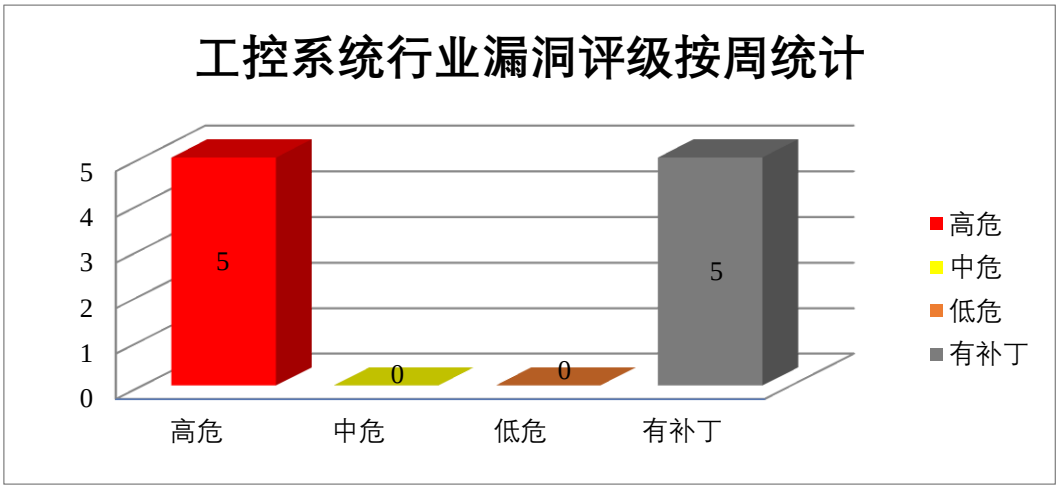

图 5 工控系统行业漏洞统计

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、DELL 产品安全漏洞

Dell PowerPath Management Appliance 是美国戴尔（Dell）公司的一种 PowerPath 主机管理应用程序，提供两种模型：基于虚拟机的设备和 Docker 容器化设备。Dell PowerScale OneFS 是一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。Dell BIOS 是一个计算机主板上小型内存芯片上的嵌入式软件。Dell EMC Metro node 是一个除数据中心内部、跨数据中心和数据中心之间的物理障碍的应用程序。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数据，通过发送恶意的 HTTP 或 HTTPS 请求以 root 用户权限执行任意的 shell 命令，覆盖任意文件从而导致拒绝服务等。

CNVD 收录的相关漏洞包括：Dell PowerPath Management Appliance 授权问题漏洞、Dell PowerScale OneFS 资源管理错误漏洞、Dell PowerScale OneFS 授权问题漏洞（CNVD-2023-14503）、Dell BIOS 输入验证错误漏洞（CNVD-2023-14507、CNVD-2023-14506）、Dell EMC Metro node 代码注入漏洞、Dell BIOS 缓冲区溢出漏洞（CNVD-2023-14511）、Dell PowerScale OneFS 信息泄露漏洞（CNVD-2023-16362）。其中，“Dell PowerPath Management Appliance 授权问题漏洞、Dell EMC Metro node 代码注入漏洞”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-2023-14505
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14504
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14503
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14507
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14506
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14512
https://www.cnvd.org.cn/flaw/show/CNVD-2023-14511
https://www.cnvd.org.cn/flaw/show/CNVD-2023-16362

2、Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞在受害者的浏览器上下文中执行恶意 JavaScript 代码。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2023-15822、CNVD-2023-15825、CNVD-2023-15824、CNVD-2023-15823、CNVD-2023-15828、CNVD-2023-15827、CNVD-2023-15826、CNVD-2023-15831）。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-2023-15822

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15825

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15824

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15823

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15828

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15827

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15826

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15831

3、Google 产品安全漏洞

Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。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拒绝服务。

CNVD 收录的相关漏洞包括：Google TensorFlow 输入验证错误漏洞（CNVD-2023-15776、CNVD-2023-15775、CNVD-2023-15779、CNVD-2023-15778、CNVD-2023-15777、CNVD-2023-15781、CNVD-2023-15780）、Google TensorFlow 缓冲区溢出漏洞（CNVD-2023-15774）。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-2023-15776

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15775

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15774

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15779

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15778

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15777

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15781

https://www.cnvd.org.cn/flaw/show/CNVD-2023-15780

4、Siemens 产品安全漏洞

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。Siemens Tecnomatix Plant Simulation 是面向对象的、图形化的、集成的建模、仿真工具。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解析特制的 DWG 文件在当前进程中执行代码等。

CNVD 收录的相关漏洞包括：Siemens Solid Edge 未初始化指针漏洞（CNVD-2023-15413、CNVD-2023-15420）、Siemens Solid Edge 内存破坏漏洞（CNVD-2023-15415）、Siemens Tecnomatix Plant Simulation 未初始化指针漏洞、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-15417）、CNVD-2023-15416、CNVD-2023-

15419、CNVD-2023-15418）。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-2023-15413
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15414
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15415
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15417
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15416
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15419
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15418
https://www.cnvd.org.cn/flaw/show/CNVD-2023-15420

5、ZTE ZXHN-H108NS 堆栈缓冲区溢出漏洞

ZTE ZXHN-H108NS 是中国中兴通讯（ZTE）公司的一款无线路由器。本周，ZTE ZXHN-H108NS 被披露存在堆栈缓冲区溢出漏洞。攻击者可利用此漏洞导致设备崩溃。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-2023-15762

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-2023-14998	Microsoft Word 远程代码执行漏洞（CNVD-2023-14998）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21716
CNVD-2023-15695	Tenda AC1206 堆栈溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tenda.com.cn/download/detail-2766.html
CNVD-2023-15717	Huawei HarmonyOS 安全绕过漏洞（CNVD-2023-15717）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202302-0000001454769474
CNVD-2023-15718	Huawei HarmonyO SHwContacts 模块逻辑绕过漏洞	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://device.harmonyos.com/cn/doc

			s/security/update/security-bulletins-202302-0000001454769474
CNVD-2023-15732	Huawei HarmonyOS 多屏幕协作模块权限提升漏洞	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://device.harmonyos.com/en/docs/security/update/security-bulletins-202302-0000001454769474
CNVD-2023-15763	ZTE OTCP 权限和访问控制漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026164
CNVD-2023-15782	Google TensorFlow 拒绝服务漏洞（CNVD-2023-15782）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f4w6-h4f5-wx45
CNVD-2023-15783	Google TensorFlow 拒绝服务漏洞（CNVD-2023-15783）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v5xg-3q2c-c2r4
CNVD-2023-15815	Mozilla Firefox 信任管理问题漏洞（CNVD-2023-15815）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/
CNVD-2023-15820	Mozilla Firefox 后置链接漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/

小结：本周，DELL 产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感数据，通过发送恶意的 HTTP 或 HTTPS 请求以 root 用户权限执行任意的 shell 命令，覆盖任意文件从而导致拒绝服务等。此外，Adobe、Google、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在受害者的浏览器上下文中执行恶意 JavaScript 代码，通过解析特制的 DWG 文件在当前进程中执行代码，导致拒绝服务。另外，ZXHN-H108NS 被披露存在堆栈缓冲区溢出漏洞。攻击者可利用此漏洞导致设备崩溃。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、Tenda AC23 堆栈溢出漏洞（CNVD-2023-15697）

验证描述

Tenda AC23 是中国腾达（Tenda）公司的一款双频千兆无线路由器。

Tenda AC23 存在堆栈溢出漏洞，该漏洞源于 formSetFirewallCfg 函数中的 firewallEn 参数存在堆栈溢出。攻击者可利用该漏洞执行非授权指令，可以取得系统特权，进而进行各种非法操作。

验证信息

POC 链接：https://github.com/ppcrab/IOT_FIRMWARE/blob/main/Tenda/ac23/ac23.md#fromsetwifigusetbasic

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-15697

信息提供者

深信服科技股份有限公司

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. Jenkins 开源：新的安全漏洞可允许代码执行攻击

Jenkins 开源自动化服务器中披露了两个安全漏洞，利用此漏洞可在目标系统上执行任何代码。这些漏洞被追踪为 CVE-2023-27898 和 CVE-2023-27905，影响 Jenkins 服务器和更新中心，并被云安全公司 Aqua 统称为 CorePlague。

参考链接：https://thehackernews.com/2023/03/jenkins-security-alert-new-security.html

2. Fortinet FortiOS 和 FortiProxy 存在缓冲区溢出漏洞，可导致任意代码执行

Fortinet 解决了一个存在于 FortiOS 和 FortiProxy 的管理界面中的缓冲区溢出漏洞，跟踪为 CVE-2023-25610。未经身份验证的远程攻击者可以利用该漏洞在易受攻击的设备上执行任意代码，并通过发送特制的请求在 GUI 上触发 DoS 条件。

参考链接：https://securityaffairs.com/143227/security/fortinet-fortios-fortiproxy-critical-bug.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