国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 02 月 26 日-2024 年 03 月 03 日 **2024 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 349 个，其中高危漏洞 135 个、中危漏洞 196 个、低危漏洞 18 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 251 个（占 72%），其中互联网上出现“Tenda AC 10U formSetDeviceName 函数堆栈缓冲区溢出漏洞、Yifan YF325 缓冲区溢出漏洞”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 19789 个，与上周（6129 个）环比增加 2.23 倍。

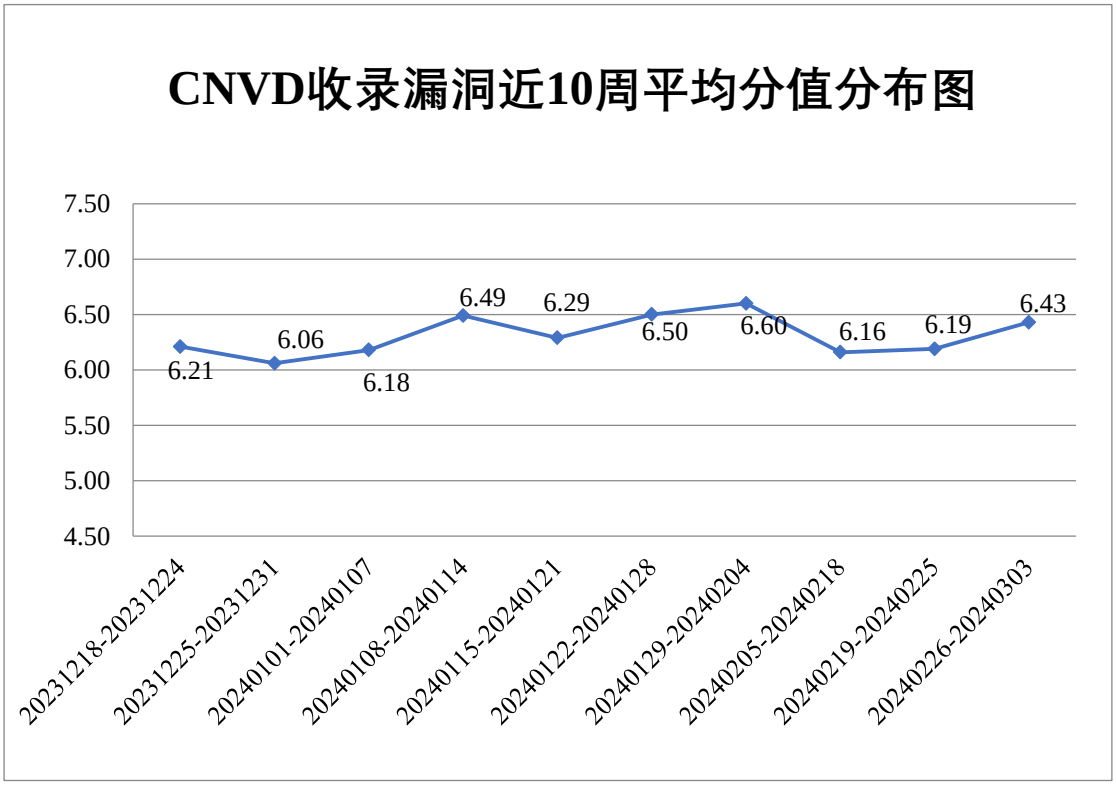

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向基础电信企业通报漏洞事件 2 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 859 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 130 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 16 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：

佐藤自动识别系统国际贸易（上海）有限公司、紫光软件系统有限公司、重庆中联信息产业有限责任公司、众安商业集团有限公司、中远麒麟科技有限公司、中国科技出版传媒股份有限公司、中国教育图书进出口有限公司、中保无限科技有限公司、智互联（深圳）科技有限公司、郑州郑大信息技术有限公司、正泰集团股份有限公司、浙江宇视科技有限公司、浙江汉脑数码科技有限公司、掌如科技服务有限公司、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、永中软件股份有限公司、兄弟（中国）商业有限公司、新道科技股份有限公司、小米科技有限责任公司、西安瑞友信息技术资讯有限公司、西安旌旗电子股份有限公司、武汉中地数码科技有限公司、武汉天喻信息产业股份有限公司、武汉海云健康科技股份有限公司、卫宁健康科技集团股份有限公司、威海市天罡仪表股份有限公司、网神信息技术（北京）股份有限公司、万洲电气股份有限公司、万州电器股份有限公司、推想医疗科技股份有限公司、腾讯安全应急响应中心、台达电子企业管理（上海）有限公司、苏州天一信德环保科技有限公司、苏州青颖飞帆软件科技股份有限公司、苏州科达科技股份有限公司、深圳市智络科技有限公司、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、深圳力维智联技术有限公司、深圳金三立视频科技股份有限公司、上海盈策信息技术有限公司、上海阳昀网络科技有限公司、上海威派格智慧水务股份有限公司、上海商派网络科技有限公司、上海企望信息科技有限公司、上海曼恒数字技术股份有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海伯俊软件科技有限公司、山西森甲能源科技有限公司、山脉科技股份有限公司、山东潍微科技股份有限公司、山东科德电子有限公司、山东比特智能科技股份有限公司、厦门亿联网络技术股份有限公司、厦门天锐科技股份有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、三星（中国）投资有限公司、青岛三利集团有限公司、青岛浩海网络科技股份有限公司、南京双日教育科技有限公司、南京功夫豆信息科技有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、辽宁省联航物流科技有限公司、浪潮数字（山东）科技有限公司、朗坤智慧科技股份有限公司、蓝网科技股份有限公司、金蝶软件（中国）有限公司、金典高科（北京）科技有限公司、江苏天瑞仪器股份有限公司、吉翁电子（深圳）有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、杭州云润科技有限公司、杭

州雄伟科技开发股份有限公司、杭州雄迈信息技术有限公司、杭州荷花软件有限公司、杭州恩软信息技术有限公司、哈尔滨伟成科技有限公司、广州市奥威亚电子科技有限公司、广联达科技股份有限公司、广东优信无限网络股份有限公司、广东省珠海迈科智能科技股份有限公司、广东飞企互联科技股份有限公司、广东保伦电子股份有限公司、福建科立讯通信有限公司、福建博思软件股份有限公司、泛微网络科技股份有限公司、帆软软件有限公司、东华软件股份公司、东莞市冬惊鱼网络科技有限公司、禅道软件（青岛）有限公司、北京中宇万通科技股份有限公司、北京智慧远景科技产业有限公司、北京致远互联软件股份有限公司、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、北京万户网络技术有限公司、北京硕人时代科技股份有限公司、北京数字政通科技股份有限公司、北京时空智友科技有限公司、北京神州视翰科技有限公司、北京派网软件有限公司、北京灵州网络技术有限公司、北京京东叁佰陆拾度电子商务有限公司、北京金和网络股份有限公司、北京和欣运达科技有限公司、北京百卓网络技术有限公司、北京安胜华信科技有限公司、安徽旭帆信息科技有限公司、爱瑞思软件（深圳）有限公司和阿里巴巴集团安全应急响应中心。

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、安天科技集团股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。贵州多彩网安科技有限公司、江苏金盾检测技术股份有限公司、联想集团、河南东方云盾信息技术有限公司、北京卓识网安技术股份有限公司、安徽天行网安信息安全技术有限公司、江苏百达智慧网络科技有限公司（含光实验室）、江苏锋刃信息科技有限公司、快页信息技术有限公司、内蒙古洞明科技有限公司、海南神州希望网络有限公司、西藏熙安信息技术有限责任公司、杭州默安科技有限公司、浙江工业大学、内蒙古中叶信息技术有限责任公司、北京时代新威信息技术有限公司、北京微步在线科技有限公司、杭州海康威视数字技术股份有限公司、星云博创科技有限公司、河南灵创电子科技有限公司、中国电信股份有限公司上海研究院、江苏天创科技有限公司、北京山石网科信息技术有限公司、杭州寻臻科技有限责任公司、湖南泛联新安信息科技有限公司、河南悦海数安科技有限公司、江苏君立华域信息安全技术股份有限公司、上海观安信息技术股份有限公司、广州安亿信软件科技有限公司、广西塔易信息技术有限公司、济南三泽信息安全测评有限公司、北京双湃智安科技有限公司、甘肃赛飞安全科技有限公司、中孚安全技术有限公司、国网上海市电力公司、深圳昂楷科技有限公司、蚂蚁集团（AFS）、广州中科诺泰技术有限公司、贵州电网有限责任公司信息中心、青海祥润网络科技有限公司、沈阳化工大学-辽宁省石油化工行业信息安全重点实验室、山东云天安全技术有限公司、北京墨云科技有限公司、信联科技（南

京）有限公司、山石网科通信技术股份有限公司、吉林省吉林祥云信息技术有限公司、北京天防安全科技有限公司、赛尔网络有限公司、南京深安科技有限公司、南京共美科技有限公司、成都安美勤信息技术股份有限公司、江苏极元信息技术有限公司、成都愚安科技有限公司及其他个人白帽子向 CNVD 提交了 19789 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 15089 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	原创漏洞数量
斗象科技（漏洞盒子）	11975	11975
奇安信网神（补天平台）	1611	1611
上海交大	937	937
新华三技术有限公司	762	0
深信服科技股份有限公司	620	22
三六零数字安全科技集团有限公司	566	566
安天科技集团股份有限公司	299	0
北京神州绿盟科技有限公司	248	1
北京数字观星科技有限公司	204	0
阿里云计算有限公司	164	0
天津市国瑞数码安全系统股份有限公司	92	0
北京启明星辰信息安全技术有限公司	89	7
杭州安恒信息技术股份有限公司	81	12
北京安信天行科技有限公司	68	68
北京知道创宇信息技术有限公司	61	1
恒安嘉新（北京）科	60	0

技股份公司		
杭州迪普科技股份有限公司	10	0
远江盛邦（北京）网络安全科技股份有限公司	9	9
北京长亭科技有限公司	9	9
南京联成科技发展股份有限公司	4	4
中国电信集团系统集成有限责任公司	3	3
北京智游网安科技有限公司	3	3
北京天融信网络安全技术有限公司	2	2
西安四叶草信息技术有限公司	1	1
贵州多彩网安科技有限公司	140	140
江苏金盾检测技术股份有限公司	127	127
联想集团	58	58
河南东方云盾信息技术有限公司	31	31
北京卓识网安技术股份有限公司	28	28
安徽天行网安信息安全技术有限公司	25	25
江苏百达智慧网络科技有限公司（含光实验室）	17	17
江苏锋刃信息科技有限公司	12	12
快页信息技术有限公	10	10

司		
内蒙古洞明科技有限公司	10	10
海南神州希望网络有限公司	10	10
西藏熙安信息技术有限责任公司	8	8
杭州默安科技有限公司	7	7
浙江工业大学	6	6
内蒙古中叶信息技术有限责任公司	5	5
北京时代新威信息技术有限公司	5	5
北京微步在线科技有限公司	5	5
杭州海康威视数字技术股份有限公司	5	5
星云博创科技有限公司	5	5
河南灵创电子科技有限公司	5	5
中国电信股份有限公司上海研究院	5	5
江苏天创科技有限公司	4	4
北京山石网科信息技术有限公司	4	4
杭州寻臻科技有限责任公司	3	3
湖南泛联新安信息科技有限公司	3	3
河南悦海数安科技有限公司	3	3
江苏君立华域信息安	3	3

全技术股份有限公司		
上海观安信息技术股份有限公司	3	3
广州安亿信软件科技有限公司	2	2
广西塔易信息技术有限公司	2	2
济南三泽信息安全测评有限公司	2	2
北京双湃智安科技有限公司	2	2
甘肃赛飞安全科技有限公司	2	2
中孚安全技术有限公司	1	1
国网上海市电力公司	1	1
深圳昂楷科技有限公司	1	1
蚂蚁集团（AFS）	1	1
广州中科诺泰技术有限公司	1	1
贵州电网有限责任公司信息中心	1	1
青海祥润网络科技有限公司	1	1
沈阳化工大学-辽宁省石油化工行业信息安全重点实验室	1	1
山东云天安全技术有限公司	1	1
北京墨云科技有限公司	1	1
信联科技（南京）有限公司	1	1
山石网科通信技术股	1	1

份有限公司		
吉林省吉林祥云信息技术有限公司	1	1
北京天防安全科技有限公司	1	1
赛尔网络有限公司	1	1
南京深安科技有限公司	1	1
南京共美科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
江苏极元信息技术有限公司	1	1
成都愚安科技有限公司	1	1
CNCERT 宁夏分中心	4	4
CNCERT 内蒙古分中心	4	4
个人	1326	1326
报送总计	19789	17142

本周漏洞按类型和厂商统计

本周，CNVD 收录了 349 个漏洞。WEB 应用 214 个，应用程序 70 个，网络设备（交换机、路由器等网络端设备）35 个，数据库 14 个，操作系统 10 个，智能设备（物联网终端设备）6 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	214
应用程序	70
网络设备（交换机、路由器等网络端设备）	35
数据库	14
操作系统	10
智能设备（物联网终端设备）	6

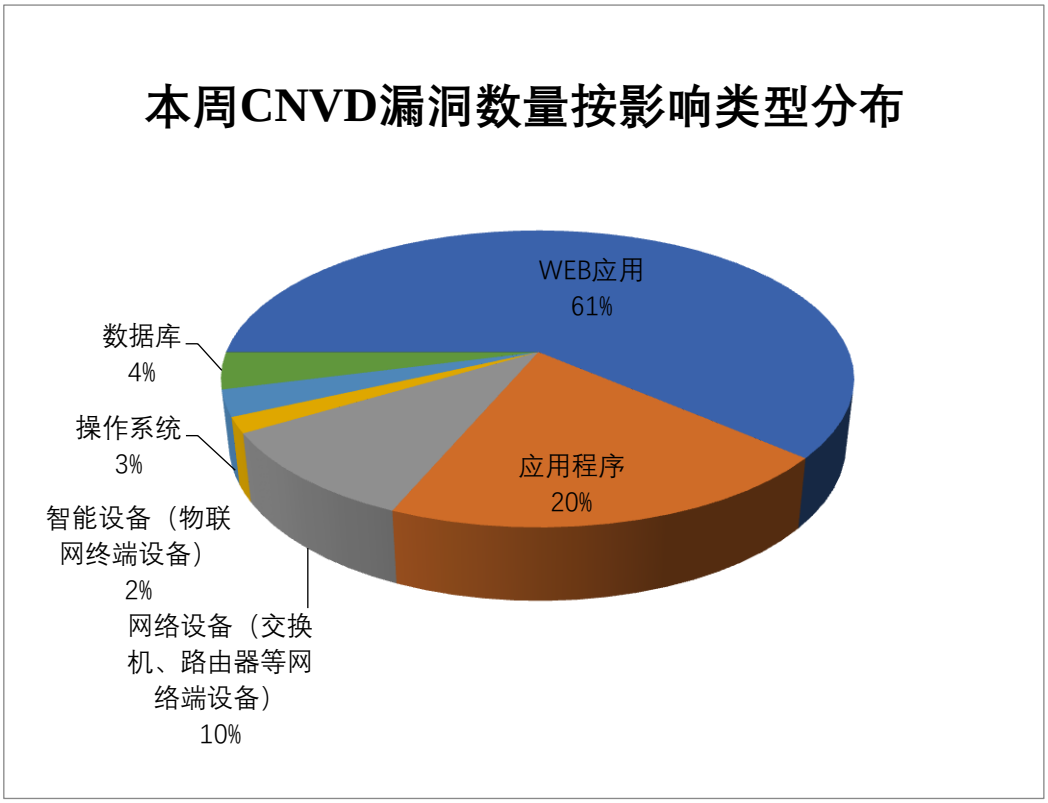

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cups Easy、Google、Mozilla 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	Cups Easy	27	8%
2	Google	21	6%
3	Mozilla	15	4%
4	北京星网锐捷网络技术有限公司	13	4%
5	Oracle	12	3%
6	IBM	11	3%
7	用友网络科技股份有限公司	11	3%
8	SAP	10	3%
9	Tenda	6	2%
10	其他	223	64%

本周行业漏洞收录情况

本周，CNVD 收录了 43 个电信行业漏洞，27 个移动互联网行业漏洞，7 个工控行

业漏洞（如下图所示）。其中，“TOTOLINK A3300R setMacFilterRules 方法命令注入漏洞、Google Android 权限提升漏洞（CNVD-2024-10417）”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/

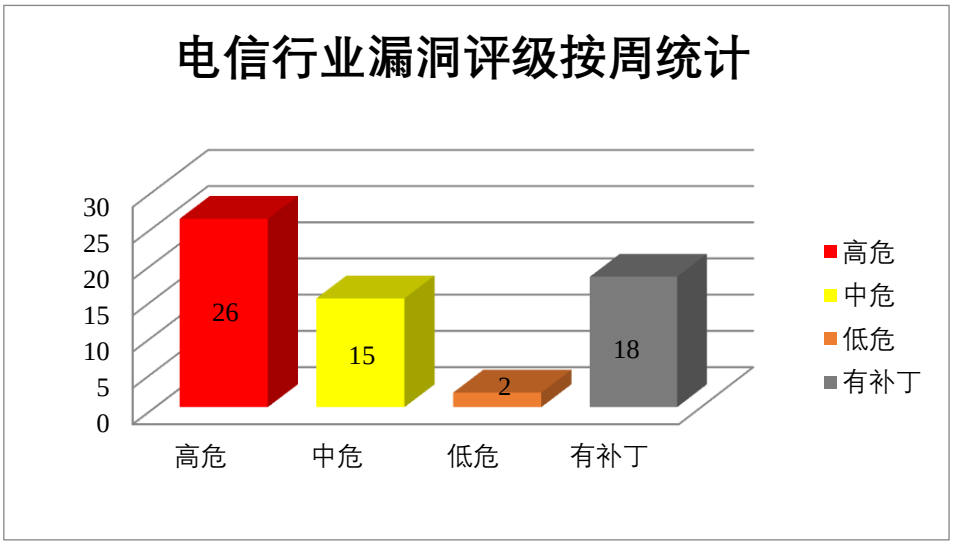

图 3 电信行业漏洞统计

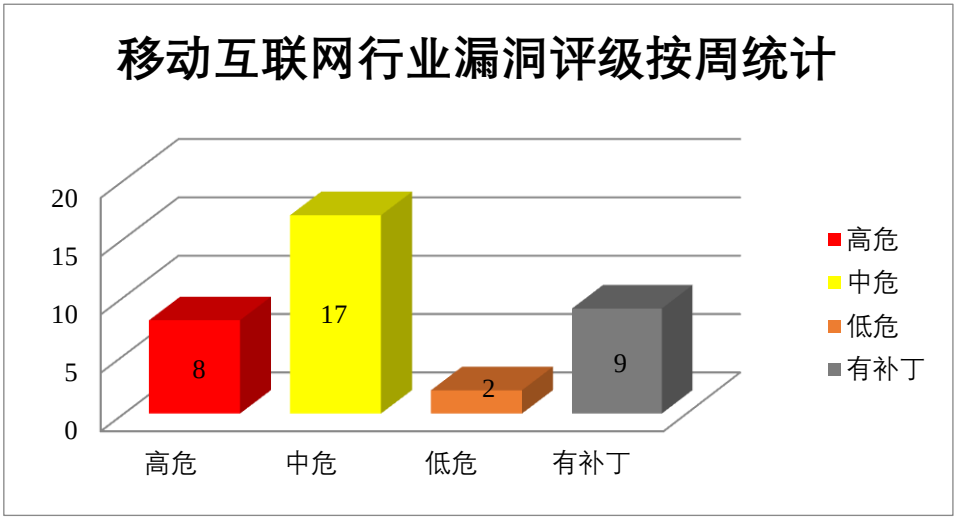

图 4 移动互联网行业漏洞统计

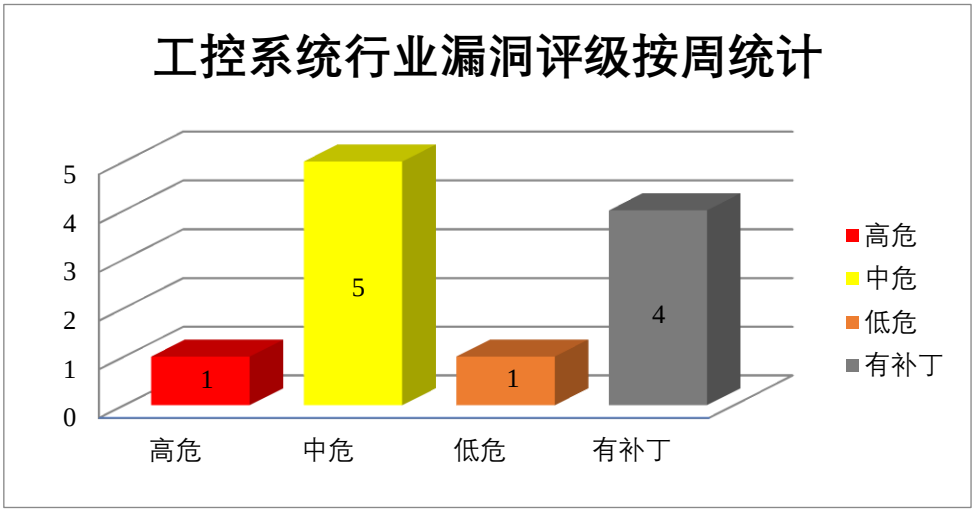

图 5 工控系统行业漏洞统计

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。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得提升的权限，在系统上执行任意代码，或者导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome 堆缓冲区溢出漏洞（CNVD-2024-10412）、Google Chrome 内存错误引用漏洞（CNVD-2024-10413、CNVD-2024-10414、CNVD-2024-10415）、Google Android 权限提升漏洞（CNVD-2024-10417、CNVD-2024-10418、CNVD-2024-10423）、Google Android 代码执行漏洞（CNVD-2024-10419）。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-2024-10412

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10413

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10414

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10415

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10417

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10418

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10419

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10423

2、 IBM 产品安全漏洞

IBM PowerSC 是美国国际商业机器（IBM）公司的一款用于 IBM Power Systems 服务器的安全和合规性解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞暴力破解帐户凭据，访问未经授权的用户，注入恶意的 HTML 代码等。

CNVD 收录的相关漏洞包括：IBM PowerSC 加密问题漏洞（CNVD-2024-09945）、IBM PowerSC 跨站脚本漏洞、IBM PowerSC 点击劫持漏洞、IBM PowerSC 信息泄露漏洞（CNVD-2024-09941、CNVD-2024-09950）、IBM PowerSC 会话固定漏洞（CNVD-2024-09948、CNVD-2024-09951）、IBM PowerSC 认证错误漏洞。其中，“IBM PowerSC 信息泄露漏洞（CNVD-2024-09950）”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-2024-09945
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09943
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09942
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09941
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09948
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09947
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09951
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09950

3、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏览器）的一个延长支持版本。Mozilla Thunderbird 是电子邮件客户端软件，支持 IMAP、POP 邮件协议以及 HTML 邮件格式。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，在系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品代码执行漏洞、Mozilla Firefox 拒绝服务漏洞（CNVD-2024-10431、CNVD-2024-10432、CNVD-2024-10435、CNVD-2024-10437）、多款 Mozilla 产品安全绕过漏洞（CNVD-2024-10434）、多款 Mozilla 产品权限提升漏洞（CNVD-2024-10433）、多款 Mozilla 产品拒绝服务漏洞。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-2024-10430
https://www.cnvd.org.cn/flaw/show/CNVD-2024-10431
https://www.cnvd.org.cn/flaw/show/CNVD-2024-10432
https://www.cnvd.org.cn/flaw/show/CNVD-2024-10434
https://www.cnvd.org.cn/flaw/show/CNVD-2024-10433
https://www.cnvd.org.cn/flaw/show/CNVD-2024-10435

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10437

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10436

4、SAP 产品安全漏洞

SAP Companion 是德国思爱普（SAP）公司的一款 SAP 的协同服务器。SAP ABA (Application Basis) 是一款由 SAP 开发的应用事务管理系统。SAP IDES Systems 是德国思爱普（SAP）公司的一款交互式演示与教育系统。SAP Cloud Connector 是德国思爱普（SAP）公司的一个工具，用于建立本地系统与 SAP Cloud Platform 之间的安全连接。SAP S/4HANA 是德国思爱普（SAP）公司的一个基于 SAP HANA 内存数据库系统的的企业资源管理软件。SAP NetWeaver ABAP Server 是德国思爱普（SAP）公司的一个用作 SAP 产品的 Web 应用程序服务器。SAP NetWeaver AS 是德国思爱普（SAP）公司的一款 SAP 网络应用服务器。它不仅能提供网络服务，且还是 SAP 软件的基本平台。SAP Application Interface Framework（SAP AIF）是德国思爱普（SAP）公司的一个应用程序接口框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得对数据的访问权限，执行任意代码，导致权限升级等。

CNVD 收录的相关漏洞包括：SAP Companion 跨站脚本漏洞、SAP ABA 代码注入漏洞、SAP IDES Systems 命令注入漏洞、SAP Cloud Connector 信任管理问题漏洞（CNVD-2024-10198）、SAP S/4HANA 授权问题漏洞（CNVD-2024-10202）、SAP NetWeaver ABAP Server 跨站脚本漏洞（CNVD-2024-10201）、SAP NetWeaver AS 跨站脚本漏洞（CNVD-2024-10206）、SAP Application Interface Framework 跨站脚本漏洞。其中，“SAP ABA 代码注入漏洞、SAP Cloud Connector 信任管理问题漏洞（CNVD-2024-10198）” 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-2024-10197

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10200

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10199

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10198

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10202

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10201

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10206

https://www.cnvd.org.cn/flaw/show/CNVD-2024-10205

5、Hyperledger Ursa 信息泄露漏洞

Hyperledger Ursa 是 Hyperledger 开源的一个与区块链一起使用的密码库。本周，Hyperledger Ursa 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取敏感信息。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-2024-10428

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-2024-09950	IBM PowerSC 信息泄露漏洞（CNVD-2024-09950）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7113759
CNVD-2024-10200	SAP ABA 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/february-2024.html
CNVD-2024-10417	Google Android 权限提升漏洞（CNVD-2024-10417）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7
CNVD-2024-10429	Microsoft Office 远程代码执行漏洞（CNVD-2024-10429）	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-2024-20673
CNVD-2024-10441	多款 Mozilla 产品安全绕过漏洞（CNVD-2024-10441）	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/mfsa2024-01/
CNVD-2024-10444	多款 Mozilla 产品拒绝服务漏洞（CNVD-2024-10444）	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/mfsa2024-01/
CNVD-2024-10467	TOTOLINK A3300R setPortForwardRules 方法命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html
CNVD-2024-10466	TOTOLINK A3300R setParentalRules 方法命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/i

			ds/36.html
CNVD-2024-10471	Cisco Unity Connection 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD
CNVD-2024-10469	Cisco Unified Communications Products 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞获得提升的权限，在系统上执行任意代码，或者导致应用程序崩溃。此外，IBM、Mozilla、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获得对数据的访问权限，注入恶意的 HTML 代码，在系统上执行任意代码或导致拒绝服务等。另外，Hyperledger Ursa 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取敏感信息。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 AC10U formSetDeviceName 函数堆栈缓冲区溢出漏洞

验证描述

Tenda AC10U 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10U formSetDeviceName 函数存在堆栈缓冲区溢出漏洞，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。

验证信息

POC 链接：https://github.com/yaoyue123/iot/blob/main/Tenda/AC10U/formSetDeviceName.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-10426

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. Apple Shortcuts 中的安全漏洞可能会导致用户敏感信息泄露

网络安全公司 Bitdefender 解释说，该问题被追踪为 CVE-2024-23204，影响 iOS 和 macOS 用户，只能通过某些操作触发，但允许攻击者绕过苹果管理敏感用户信息和系统资源访问的框架。

参考链接：https://www.anquanke.com/post/id/293432

2. Windows 这个零日漏洞正在被黑客利用，以获取内核权限

研究人员近期发现，Lazarus 黑客组织正在试图利用 Windows AppLocker 驱动程序 appid.sys 中的零日漏洞（CVE-2024-21338），获得内核级访问权限并关闭安全工具，从而能够轻松绕过 BYOVD（自带漏洞驱动程序）技术。

参考链接：https://www.freebuf.com/news/392838.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