国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 04 月 08 日-2024 年 04 月 14 日 **2024 年第 15 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 376 个，其中高危漏洞 158 个、中危漏洞 201 个、低危漏洞 17 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 314 个（占 84%），其中互联网上出现“Tenda AC10U fromAddressNat 函数堆栈缓冲区溢出漏洞、Tenda AC10U fromDhcpListClient 函数堆栈缓冲区溢出漏洞”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 12440 个，与上周（6454 个）环比增加 93%。

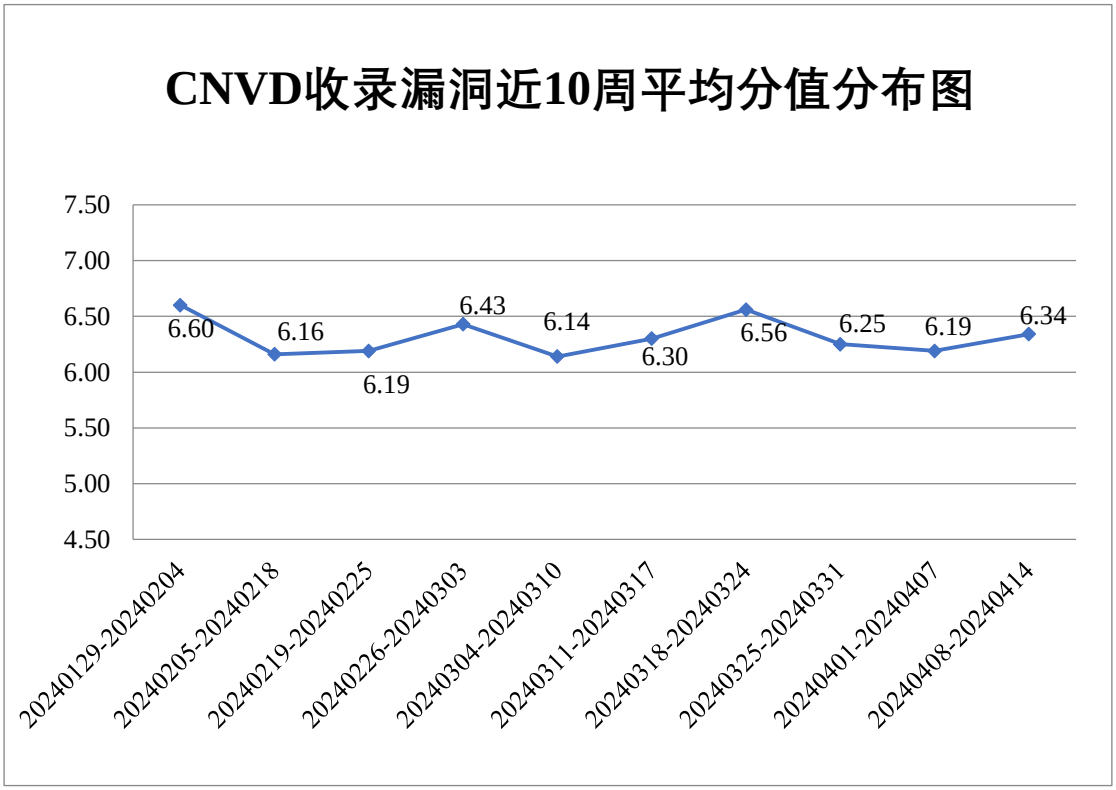

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 642 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 77 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 22 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：

重庆紫光华山智安科技有限公司、中科红旗（北京）信息科技有限公司、中葬科技有限公司、郑州意象网络科技有限公司、郑州时空智友信息技术有限公司、浙江和达科技股份有限公司、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、烟台吉安电子科技有限公司、信呼、新天科技股份有限公司、新开普电子股份有限公司、新都（青岛）电子有限公司、西安泽瑞通信有限公司、西安瑞友信息技术资讯有限公司、万洲电气股份有限公司、统信软件技术有限公司、天闻数媒科技（北京）有限公司、天维尔信息科技股份有限公司、天津市天科数创科技股份有限公司、台达电子工业股份有限公司、苏州科达科技股份有限公司、松立控股集团股份有限公司、施耐德电气（中国）有限公司、深圳拓安信物联股份有限公司、深圳市优特普技术有限公司、深圳市微笑智能有限公司、深圳市同为数码科技股份有限公司、深圳市思迅软件股份有限公司、深圳市企企通科技有限公司、深圳市力必拓科技有限公司、深圳市蓝凌软件股份有限公司、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、深圳市吉祥腾达科技有限公司、深圳市汇贤网络科技有限公司、深圳市创富港商务服务股份有限公司、深圳市步科电气有限公司、深圳锐取信息技术股份有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海易正信息技术有限公司、上海迅饶自动化科技有限公司、上海沈禄信息科技有限公司、上海瑞美电脑科技有限公司、上海肯特仪表股份有限公司、上海寰创通信科技股份有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海博达数据通信有限公司、山脉科技股份有限公司、山东潍微科技股份有限公司、山东山大华天软件有限公司、山东金钟科技集团股份有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、厦门码英网络科技有限公司、厦门快普信息技术有限公司、厦门科拓通讯技术股份有限公司、青岛三利集团有限公司、普元信息技术股份有限公司、宁波水表（集团）股份有限公司、南宁迈世信息技术有限公司、蚂蚁科技集团股份有限公司、龙蜥开源社区、龙采科技集团有限责任公司、零视技术（上海）有限公司、力创科技股份有限公司、蓝网科技股份有限公司、柯尼卡美能达集团、开放原子开源基金会、江苏省捷达科技发展有限公司、江苏冠宇科技集团有限公司、吉翁电子（深圳）有限公司、湖北楚天智能交通股份有限公司、河北先河环保科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州新视窗信息技术有限公司、杭州海康威视数字技术股份有限公司、瀚高基础软件股

份有限公司、海口快推科技有限公司、国子软件股份有限公司、广州市保伦电子有限公司、广州浩翔信息技术有限公司、广东中兴新支点技术有限公司、广东优信无限网络股份有限公司、福建科立讯通信有限公司、福建汇川物联网技术科技股份有限公司、烽火通信科技股份有限公司、东营金石软件有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、大连华天软件有限公司、成都长益西联软件有限公司、成都鹏业软件股份有限公司、畅捷通信息技术股份有限公司、常州市中环互联网信息技术有限公司、贝尔金国际有限公司、北京卓正志远软件有限公司、北京中科聚网信息技术有限公司、北京致远互联软件股份有限公司、北京优锘科技有限公司、北京永洪商智科技有限公司、北京亦谐科技有限公司、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、北京网测科技有限公司、北京万户网络技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京拓林思软件有限公司、北京硕人时代科技股份有限公司、北京神州数码云科信息技术有限公司、北京山石网科信息技术有限公司、北京三快科技有限公司、北京润乾信息系统技术有限公司、北京人大金仓信息技术股份有限公司、北京企企科技有限公司、北京联达动力信息科技股份有限公司、北京九思协同软件有限公司、北京京东叁佰陆拾度电子商务有限公司（京东）、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京安必达科技有限公司、奥琦玮信息科技（北京）有限公司、安美世纪（北京）科技有限公司、安徽旭帆信息科技有限公司、安徽微同科技有限公司、安徽省科迅教育装备有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司。

本周，CNVD 发布了《Microsoft 发布 2024 年 4 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9916

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、北京数字观星科技有限公司、北京启明星辰信息安全技术有限公司、阿里云计算有限公司、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。江苏金盾检测技术股份有限公司、中孚安全技术有限公司、河南东方云盾信息技术有限公司、中国电信股份有限公司上海研究院、快页信息技术有限公司、内蒙古中叶信息技术有限责任公司、河南灵创电子科技有限公司、北京中睿天下信息技术有限公司、北京山石网科信息技术有限公司、星云博创科技有限公司、河南宝通信息安全测评有限公司、中电万维信息技术有限责任公司、江苏极元信息技术有限公司、赛尔网络有限公司、杭州默安科技有限公司、北银金融科技有限责任公司、江苏晟晖信息科技有限公司、湖南泛联新安信息科技有限公司、江苏省公用

信息有限公司、江苏锋刃信息科技有限公司、广州万方计算机科技有限公司、北京时代新威信息技术有限公司、北京天防安全科技有限公司、北京神州泰岳软件股份有限公司、中资网络信息安全科技有限公司、安徽天行网安信息安全技术有限公司、西藏熙安信息技术有限责任公司、联通数字科技有限公司、成都安美勤信息技术股份有限公司、北京星网锐捷网络技术有限公司、杭州弘沿科技有限公司、内蒙古洞明科技有限公司、上海谋乐网络科技有限公司、江苏网擎信息技术有限公司、杭州海康威视数字技术股份有限公司、广州安亿信软件科技有限公司、北京天下信安技术有限公司、中电福富信息科技有限公司、甘肃赛飞安全科技有限公司、江苏云天网络安全技术有限公司、交通运输信息安全中心有限公司（TISEC 洪椒战队）及其他个人白帽子向 CNVD 提交了 12440 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）、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 11072 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）	8569	8569
新华三技术有限公司	1417	0
奇安信网神（补天平台）	1406	1406
三六零数字安全科技集团有限公司	634	634
北京数字观星科技有限公司	608	0
北京启明星辰信息安全技术有限公司	479	6
上海交大	463	463
阿里云计算有限公司	261	1
安天科技集团股份有限公司	219	0
北京神州绿盟科技有限公司	173	0
北京天融信网络安全技术有限公司	144	6
北京知道创宇信息技术有限公司	135	0
恒安嘉新（北京）科	103	0

技股份公司		
华为技术有限公司	65	0
远江盛邦（北京）网络安全科技股份有限公司	46	46
北京长亭科技有限公司	12	0
杭州迪普科技股份有限公司	9	0
北京安信天行科技有限公司	2	2
北京信联数安科技有限公司	2	2
北京智游网安科技有限公司	2	2
内蒙古奥创科技有限公司	1	1
江苏金盾检测技术股份有限公司	81	81
中孚安全技术有限公司	30	30
河南东方云盾信息技术有限公司	29	29
中国电信股份有限公司上海研究院	19	19
快页信息技术有限公司	16	16
内蒙古中叶信息技术有限责任公司	12	12
河南灵创电子科技有限公司	11	11
北京中睿天下信息技术有限公司	8	8
北京山石网科信息技术有限公司	6	6

星云博创科技有限公司	5	5
河南宝通信息安全测评有限公司	5	5
中电万维信息技术有限责任公司	5	5
江苏极元信息技术有限公司	4	4
赛尔网络有限公司	4	4
西门子（中国）有限公司	4	0
杭州默安科技有限公司	3	3
北银金融科技有限责任公司	3	3
江苏晟晖信息科技有限公司	3	3
湖南泛联新安信息科技有限公司	3	3
江苏省公用信息有限公司	3	3
江苏锋刃信息科技有限公司	3	3
广州万方计算机科技有限公司	3	3
北京时代新威信息技术有限公司	2	2
北京天防安全科技有限公司	2	2
北京神州泰岳软件股份有限公司	2	2
中资网络信息安全科技有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2

西藏熙安信息技术有限责任公司	2	2
联通数字科技有限公司	2	2
成都安美勤信息技术股份有限公司	1	1
北京星网锐捷网络技术有限公司	1	1
杭州弘沿科技有限公司	1	1
内蒙古洞明科技有限公司	1	1
上海谋乐网络科技有限公司	1	1
江苏网擎信息技术有限公司	1	1
杭州海康威视数字技术股份有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京天下信安技术有限公司	1	1
中电福富信息科技有限公司	1	1
甘肃赛飞安全科技有限公司	1	1
江苏云天网络安全技术有限公司	1	1
交通运输信息安全中心有限公司（TISEC 洪椒战队）	1	1
北京中关村实验室	1	1
CNCERT 山西分中心	1	1
个人	1017	1017
报送总计	16056	12440

本周漏洞按类型和厂商统计

本周，CNVD 收录了 376 个漏洞。WEB 应用 174 个，应用程序 113 个，网络设备（交换机、路由器等网络端设备）59 个，智能设备（物联网终端设备）14 个，操作系统 10 个，安全产品 3 个，车联网 2 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	174
应用程序	113
网络设备（交换机、路由器等网络端设备）	59
智能设备（物联网终端设备）	14
操作系统	10
安全产品	3
车联网	2
数据库	1

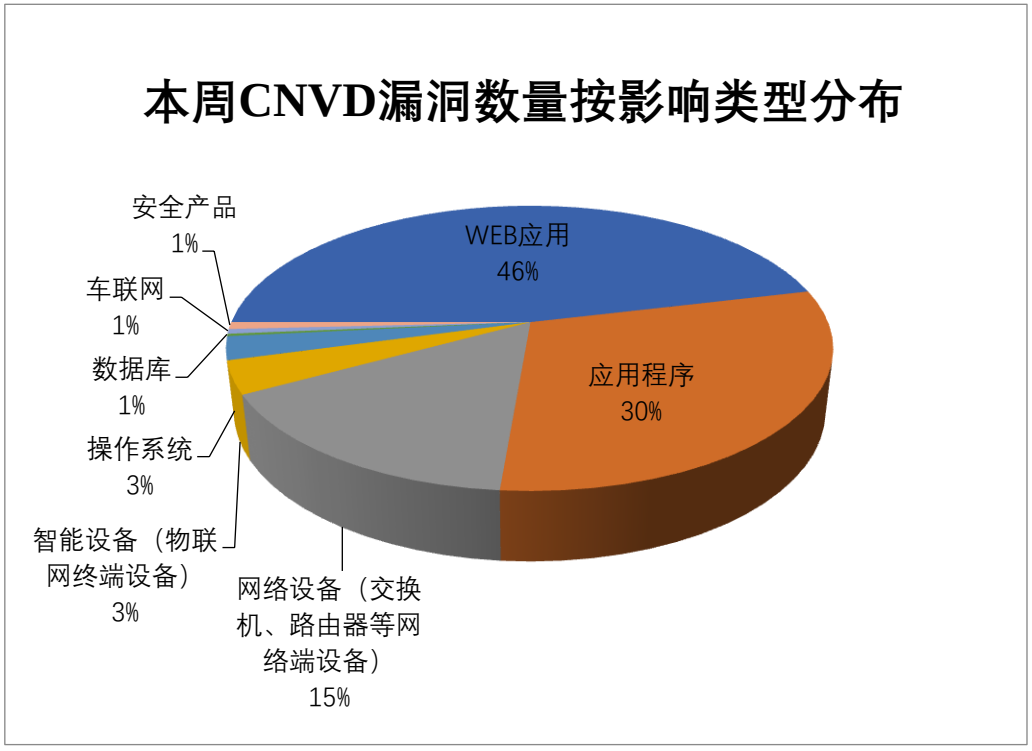

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京星网锐捷网络技术有限公司、Google、北京百卓网络技术有限公司等多家厂商的产品，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	北京星网锐捷网络技术有	17	4%

	限公司		
2	Google	13	3%
3	北京百卓网络技术有限公司	12	3%
4	Foxit	11	3%
5	用友网络科技股份有限公司	11	3%
6	DELL	10	3%
7	IBM	10	3%
8	新华三技术有限公司	7	2%
9	哈尔滨新中新电子股份有限公司	6	2%
10	其他	279	74%

本周行业漏洞收录情况

本周，CNVD 收录了 34 个电信行业漏洞，45 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，“Google Android 代码执行漏洞（CNVD-2024-16883）、Google Android 权限提升漏洞（CNVD-2024-16894）”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/

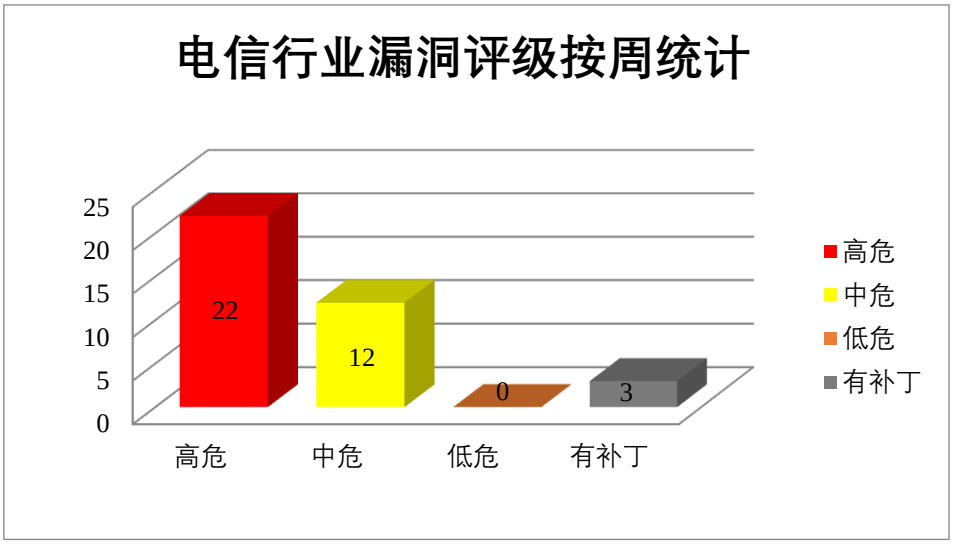

图 3 电信行业漏洞统计

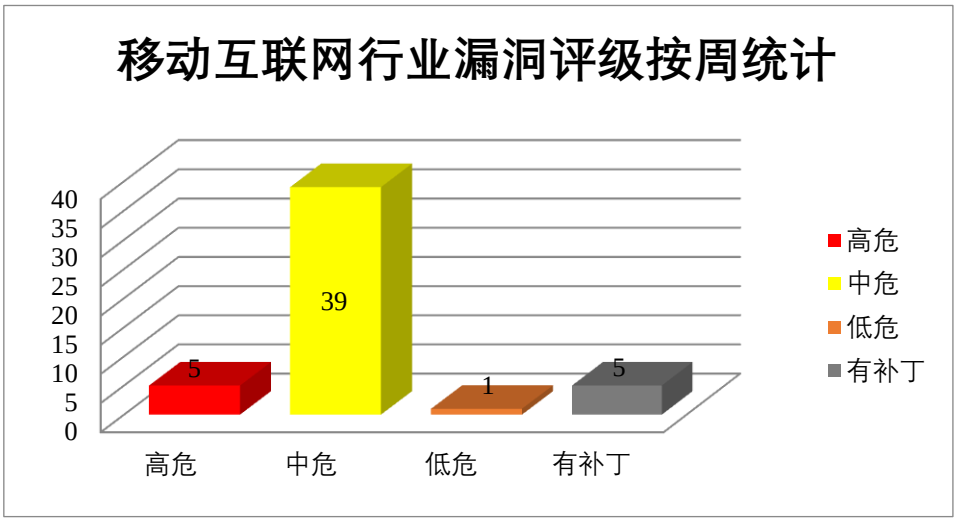

图 4 移动互联网行业漏洞统计

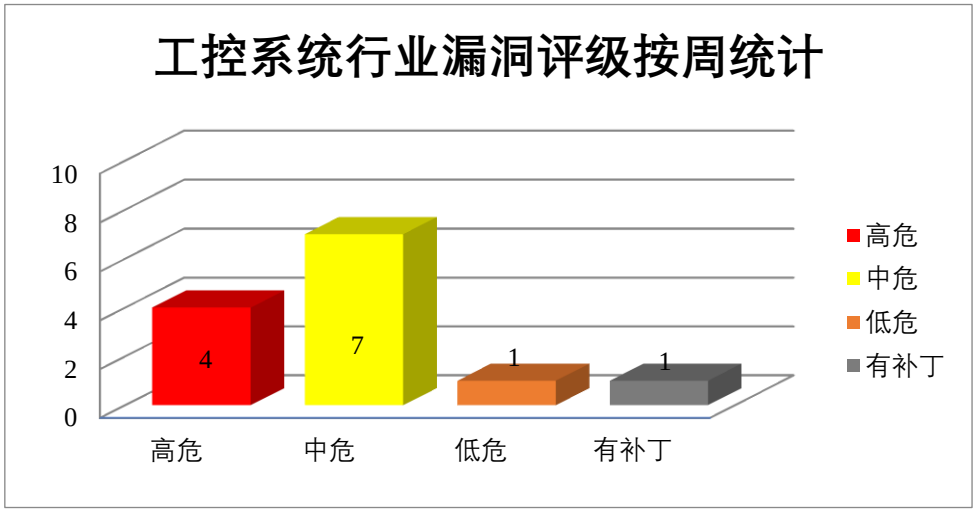

图 5 工控系统行业漏洞统计

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，攻击者可利用漏洞绕过安全限制，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 Chrome 安全绕过漏洞（CNVD-2024-16875、CNVD-2024-16881）、Google Chrome 代码执行漏洞（CNVD-2024-16876、CNVD-2024-16880、CNVD-2024-16883、CNVD-2024-16937）、Google Chrome 信息泄露漏洞（CNVD-2024-16879）、Google Android 权限提升漏洞（CNVD-2024-16882）。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-2024-16875
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16876
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16879
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16880
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16881
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16882
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16883
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16937

2、 Dell 产品安全漏洞

Dell PowerProtect Data Manager（PPDM）是美国戴尔（Dell）公司的一套数据保护解决方案。该产品支持数据备份、虚拟机备份和数据库保护等功能。Dell OpenManage Enterprise 是美国戴尔（Dell）公司的一款用于 IT 基础架构管理的易于使用的一对多系统管理控制台。Dell vApp Manager 是美国戴尔（Dell）公司的一个虚拟应用程序管理器。Dell ECS 是美国戴尔（Dell）公司的一款可扩展、易于管理且具有弹性的企业级对象存储解决方案。Dell BSAFE Micro Edition Suite 是美国戴尔（Dell）公司的一个可为 c/c++应用、设备、系统提供加密、证书和传输层安全性的开发工具包。Dell PowerScale OneFS 是美国戴尔（Dell）公司的一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。Dell NetWorker 是美国戴尔（Dell）公司的一个应用程序。提供戴尔公司的论坛讨论功能。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，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Dell OpenManage Enterprise 路径遍历漏洞、Dell PowerProtect Data Manager XML 外部实体注入漏洞、Dell vApp Manager 操作系统命令注入漏洞（CNVD-2024-16927、CNVD-2024-16928）、Dell ECS 不正确访问控制漏洞、Dell BSAFE Micro Edition Suite 信息泄露漏洞、Dell PowerScale OneFS 权限提升漏洞（CNVD-2024-16933）、Dell NetWorker 信息泄露漏洞。其中，“Dell vApp Manager 操作系统命令注入漏洞（CNVD-2024-16927、CNVD-2024-16928）、Dell ECS 不正确访问控制漏洞、Dell BSAFE Micro Edition Suite 信息泄露漏洞”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-2024-16912
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16926
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16927
https://www.cnvd.org.cn/flaw/show/CNVD-2024-16928

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16930

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16931

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16933

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16934

3、IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。IBM App Connect Enterprise 是美国国际商业机器（IBM）公司的一个操作系统。IBM Integration Bus（IBM WebSphere Message Broker）是美国国际商业机器（IBM）公司的一款企业服务总线（ESB）产品。该产品为面向服务架构（SOA）环境和非 SOA 环境提供连通性和通用数据转换。IBM CICS Transaction Gateway 是美国国际商业机器（IBM）公司的一个用于企业 CICS 资产现代化的连接器。IBM Cloud Pak for Business Automation 是美国国际商业机器（IBM）公司的一组模块化的集成软件组件，专为任何混合云而构建，旨在实现工作自动化和加速业务增长。IBM Security Verify Directory 是美国国际商业机器（IBM）公司的一款身份验证和访问管理解决方案的一部分。IBM Storage Protect Plus Server 是美国国际商业机器（IBM）公司的一款 IBM Storage 软件，可为虚拟机、数据库、应用程序、文件系统、SaaS 工作负载和容器提供恢复、复制、保留和复用功能。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等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 日志信息泄露漏洞、IBM App Connect Enterprise and IBM Integration Bus for z/OS 信息泄露漏洞、IBM CICS Transaction Gateway for Multiplatforms 信息泄露漏洞、IBM Cloud Pak for Business Automation 访问控制错误漏洞（CNVD-2024-16917）、IBM Security Verify Directory 信息泄露漏洞（CNVD-2024-16925、CNVD-2024-16924）、IBM Storage Protect Plus Server 信息泄露漏洞（CNVD-2024-16923）、IBM Storage Protect Plus Server 访问控制错误漏洞。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-2024-16920

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16919

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16918

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16917

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16925

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16924

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16923

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16922

4、Foxit 产品安全漏洞

Foxit Reader 和 Foxit PhantomPDF 都是中国福昕（Foxit）公司的一款 PDF 文档阅读器。Foxit PDF Editor 是一款 PDF 编辑器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞写入任意文件，在系统上执行代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 和 PDF Editor 代码执行漏洞、Foxit PDF Reader Doc Object 代码执行漏洞、Foxit PDF Reader AcroForm Annotation 类型混淆代码执行漏洞、Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2024-17009）、Foxit PDF Reader 远程代码执行漏洞（CNVD-2024-17008）、Foxit PDF Reader AcroForm 代码执行漏洞（CNVD-2024-17007、CNVD-2024-17006）、Foxit Reader 和 Foxit PhantomPDF 任意文件写入漏洞。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-2024-16874
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17005
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17004
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17009
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17008
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17007
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17006
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17012

5、Technicolor TC8715D 跨站脚本漏洞

Technicolor TC8715D 是法国特艺（Technicolor）公司的一个无线路由器。本周，Technicolor TC8715D 被披露存在跨站脚本漏洞。攻击者可利用该漏洞获取用户 cookie 等敏感信息。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-2024-16939

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-2024-16894	Google Android 权限提升漏洞（CNVD-2024-16894）	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://source.android.com/docs/security/bulletin/pixel/2022-12-01
CNVD-2024-16874	Foxit PDF Reader 和 PDF Editor 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.foxit.com/support/security-bulletins.html
CNVD-2024-16880	Google Chrome 代码执行漏洞（CNVD-2024-16880）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html
CNVD-2024-16928	Dell vApp Manager 操作系统命令注入漏洞（CNVD-2024-16928）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000223609/dsa-2024-108-dell-powermaxos-5978-dell-powermax-os-10-0-1-5-dell-powermax-os-10-1-0-2-dell-unisphere-360-unisphere-powermax-unisphere-powermax-vapp-dell-solutions-enabler-vapp-and-dell-powermax-eem-security-update-for-multiple-vulnerabilities
CNVD-2024-16936	Google Chrome 安全绕过漏洞（CNVD-2024-16936）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
CNVD-2024-17007	Foxit PDF Reader AcroForm 代码执行漏洞（CNVD-2024-17007）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html
CNVD-2024-17299	Siemens Parasolid 越界读取漏洞（CNVD-2024-17299）	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-222019.html
CNVD-2024-16937	Google Chrome 代码执行漏洞（CNVD-2024-16937）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
CNVD-2024-17821	Citrix NetScaler ADC 和 Gateway 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549
CNVD-2024-16882	Google Android 权限提升漏洞（CNVD-2024-16882）	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/2024-03-01

小结：本周，Google 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，获取敏感信息，提升权限，在系统上执行任意代码。此外，Dell、IBM、Foxit 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，写入任意文件，在系统上执行任意代码，导致拒绝服务等。另外，Technicolor TC8715D 被披露存在跨站脚本漏洞。攻击者可利用漏洞获取用户 cookie 等敏感信息。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 fromAddressNat 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 15.03.06.49_multi_TDE01 版本存在缓冲区溢出漏洞，该漏洞源于 fromAddressNat 函数的 Entrys/mitInterface/page 参数未能正确验证输入数据的长度大小，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/fromAddressNat_1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-16941

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. 微软修复服务器安全问题：未设密码，存储的必应关键数据可被公开访问

网络安全组织 SOCRadar 近日向微软通报了存在于 Azure 存储服务器中的安全漏洞，其存储的必应数据可以被公开访问。存在问题的 Azure 服务器主要存储微软必应（Bing）搜索相关的重要内部数据，但该服务器没有任何密码保护，因此任何网民都可以访问该服务器。

参考链接：https://www.ithome.com/0/761/141.htm

2. Spectre 漏洞 v2 版本再现，影响英特尔 CPU+Linux 组合设备

近日，网络安全研究人员披露了针对英特尔系统上 Linux 内核的首个原生 Spectre v2 漏洞，该漏洞是 2018 年曝出的处理器“幽灵”（Spectre）漏洞 v2 衍生版本，利用该漏洞可以从内存中读取敏感数据，主要影响英特尔处理器+Linux 发行版组合设备。

参考链接：https://www.freebuf.com/news/397580.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