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 05 日-2024 年 02 月 18 日　　**2024 年第 6、7 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 517 个，其中高危漏洞 188 个、中危漏洞 305 个、低危漏洞 24 个。漏洞平均分值为 6.16。本周收录的漏洞中，涉及 0day 漏洞 438 个（占 85%），其中互联网上出现“Yifan YF325 cgi_handler 函数缓冲区溢出漏洞、Yifan YF325 gozila_cgi 函数缓冲区溢出漏洞”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 7723 个，与上周（13040 个）环比减少 41%。

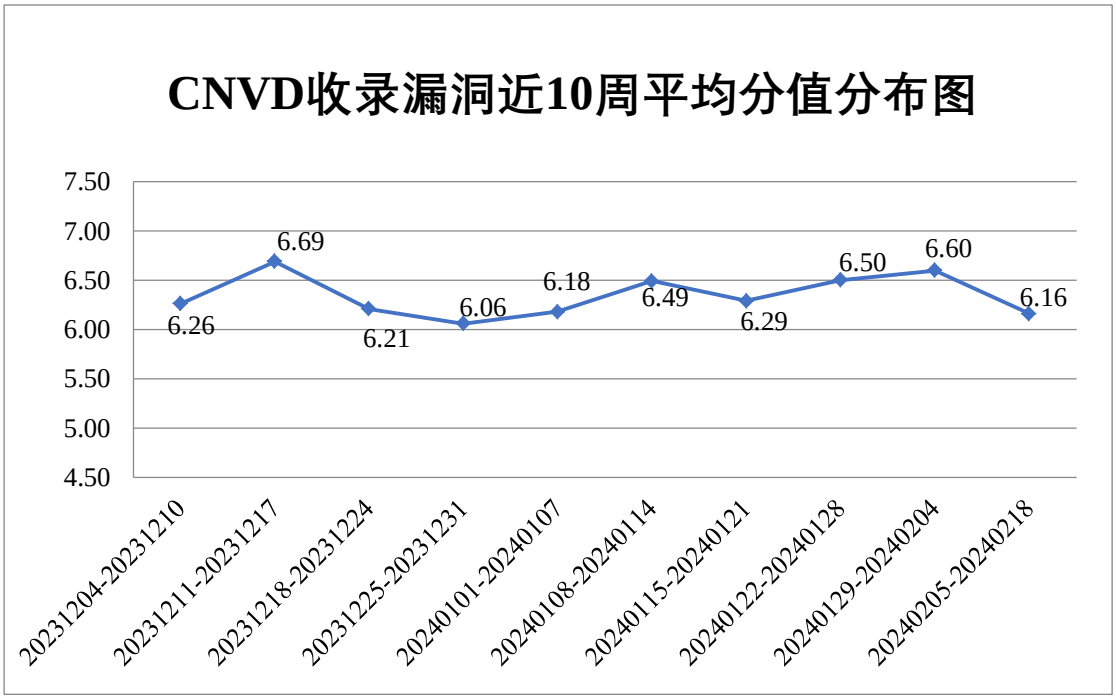

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电

信企业通报漏洞事件 6 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 335 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 54 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 42 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：

阿维塔科技（重庆）有限公司、爱普生（中国）有限公司、安科瑞电气股份有限公司、安美世纪（北京）科技有限公司、百度安全应急响应中心、百望股份有限公司、百望金赋科技有限公司、北京百卓网络技术有限公司、北京国基科技股份有限公司、北京合众思壮科技股份有限公司、北京和欣运达科技有限公司、北京宏景世纪软件股份有限公司、北京惠朗时代科技有限公司、北京金和网络股份有限公司、北京九思协同软件有限公司、北京龙软科技股份有限公司、北京魔方恒久软件有限公司、北京勤云科技发展有限公司、北京趣拿信息技术有限公司、阿里巴巴集团安全应急响应中心、阿里云计算有限公司、北京数字政通科技股份有限公司、北京通达信科科技有限公司、北京万户软件技术有限公司、北京万户网络技术有限公司、北京万维盈创科技发展有限公司、北京微瑞集智科技有限公司、北京五指互联科技有限公司、北京星网锐捷网络技术有限公司、北京星云互联科技有限公司、北京亿赛通科技发展有限责任公司、北京易普行科技有限公司、北京永洪商智科技有限公司、北京云中融信网络科技有限公司、北京致远互联软件股份有限公司、北京中成科信科技发展有限公司、北京卓软在线信息技术有限公司、北京子在川上科技有限公司、比亚迪股份有限公司、畅捷通信息技术股份有限公司、承德热力集团有限责任公司、大连华天软件有限公司、东软集团股份有限公司、福建科立讯通信有限公司、广东保伦电子股份有限公司、广联达科技股份有限公司、广州市奥威亚电子科技有限公司、广州市保伦电子有限公司、广州市动景计算机科技有限公司、广州市长远软件开发有限公司、广州易达建信科技开发有限公司、杭州恩软信息技术有限公司、杭州瑞利声电技术有限公司、杭州文朝科技有限公司、杭州雄伟科技开发股份有限公司、杭州云天软件股份有限公司、合肥翰林数码科技有限公司、合肥天寻信息科技有限公司、河南合正软件有限公司、湖北京山轻工机械股份有限公司、湖南华辰智通科技有限公司、华硕电脑（上海）有限公司、惠普贸易（上海）有限公司、吉翁电子（深圳）有限公司、济南爱程网络科技有限公司、佳能（中国）有限公司、江苏金智教育信息股份有限公司、江苏天瑞仪器股份有限公司、江苏天长环保科技有限公司、江苏欣动信息科技有限公司、金蝶软件（中国）有限公司、金山软件股份有限公司、卡莱特云科技股份有限公司、柯尼卡美能达（中国）投资有限公司、蓝网科技股份有限公司、联奕科技股份有限公司、领航未来（北京）科技有限公司、龙采科技集团有限责任公司、珞石(北京)机器人有限公司、南京恒点信息技术有限公司、鹏为软件股份有限公司、普莱德科技股份有限公司、普联技术有限公司、普元信息技术股份有限公司、奇安信网神信

息技术（北京）股份有限公司、麒麟软件有限公司、桥西区雪洛软件开发工作室、确信信息股份有限公司、任子行网络技术股份有限公司、三星（中国）投资有限公司、厦门科拓通讯技术股份有限公司、厦门亿联网络技术股份有限公司、山东科德电子有限公司、山东潍微科技股份有限公司、上海百胜软件股份有限公司、上海伯俊软件科技有限公司、上海华测导航技术股份有限公司、上海寰创通信科技股份有限公司、上海三高计算机中心股份有限公司、上海甄云科技信息有限公司、上海卓卓网络科技有限公司、深电能科技集团有限公司、深圳古瑞瓦特科技能源有限责任公司、深圳市博思高科技有限公司、深圳市吉祥腾达科技有限公司、深圳市思迅软件股份有限公司、深圳市信锐网科技术有限公司、深圳市星桐科技有限公司、深圳维盟科技股份有限公司、神州数码控股有限公司、沈阳点动科技有限公司、盛威时代科技股份有限公司、世邦通信股份有限公司、四平市九州易通科技有限公司、苏州科达科技股份有限公司、苏州寻息电子科技有限公司、腾讯安全应急响应中心、天地（常州）自动化股份有限公司、天津百望金赋科技有限公司、天津卓宏乐远信息科技有限公司、万洲电气股份有限公司、威海市天罡仪表股份有限公司、唯智信息技术（上海）股份有限公司、武汉达梦数据库股份有限公司、武汉今客软件有限公司、西安交大捷普网络科技有限公司、西安瑞友信息技术资讯有限公司、西安西瑞控制技术股份有限公司、西安众邦网络科技有限公司、西域智慧供应链（上海）股份公司、用友网络科技股份有限公司、友讯电子设备（上海）有限公司、云网软件、长沙米拓信息技术有限公司、浙江大华技术股份有限公司、浙江和达科技股份有限公司、浙江宇视科技有限公司、智恒科技股份有限公司、重庆梅安森科技股份有限公司、珠海金山办公软件有限公司、株洲田心信息技术有限公司、卓豪（中国）技术有限公司和淄博闪灵网络科技有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京数字观星科技有限公司、阿里云计算有限公司、安天科技集团股份有限公司、恒安嘉新（北京）科技股份公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。快页信息技术有限公司、河南东方云盾信息技术有限公司、内蒙古洞明科技有限公司、江苏云天网络安全技术有限公司、江苏晟晖信息科技有限公司、贵州多彩网安科技有限公司、江苏百达智慧网络科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、西藏熙安信息技术有限责任公司、深圳昂楷科技有限公司、杭州默安科技有限公司、中孚安全技术有限公司、河南悦海数安科技有限公司、安全邦（北京）信息技术有限公司、江苏君立华域信息安全技术股份有限公司、山石网科通信技术股份有限公司、统信软件技术有限公司及其他个人白帽子向 CNVD 提交了 7723 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 6530 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）	3720	3720
上海交大	2081	2081
奇安信网神（补天平台）	729	729
北京数字观星科技有限公司	386	0
阿里云计算有限公司	142	0
安天科技集团股份有限公司	60	0
恒安嘉新（北京）科技股份公司	60	0
新华三技术有限公司	51	0
北京天融信网络安全技术有限公司	31	0
中国电信集团系统集成有限责任公司	20	0
杭州迪普科技股份有限公司	8	0
西安四叶草信息技术有限公司	3	3
北京智游网安科技有限公司	2	2
北京安信天行科技有限公司	1	1
快页信息技术有限公司	22	22
河南东方云盾信息技术有限公司	18	18
内蒙古洞明科技有限公司	14	14
江苏云天网络安全技术有限公司	9	9
江苏晟晖信息科技有	7	7

限公司		
贵州多彩网安科技有限公司	7	7
江苏百达智慧网络科技有限公司	6	6
奇安星城网络安全运营服务（长沙）有限公司	4	4
西藏熙安信息技术有限责任公司	2	2
深圳昂楷科技有限公司	2	2
杭州默安科技有限公司	2	2
中孚安全技术有限公司	1	1
河南悦海数安科技有限公司	1	1
安全邦（北京）信息技术有限公司	1	1
江苏君立华域信息安全技术股份有限公司	1	1
山石网科通信技术股份有限公司	1	1
统信软件技术有限公司	1	1
CNCERT 广西分中心	2	2
CNCERT 河北分中心	1	1
个人	1085	1085
报送总计	8481	7723

本周漏洞按类型和厂商统计

本周，CNVD 收录了 517 个漏洞。WEB 应用 278 个，应用程序 115 个，网络设备（交换机、路由器等网络端设备）58 个，智能设备（物联网终端设备）25 个，操作系

统 20 个，数据库 8 个，车联网 7 个，安全产品 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	278
应用程序	115
网络设备（交换机、路由器等网络端设备）	58
智能设备（物联网终端设备）	25
操作系统	20
数据库	8
车联网	7
安全产品	6

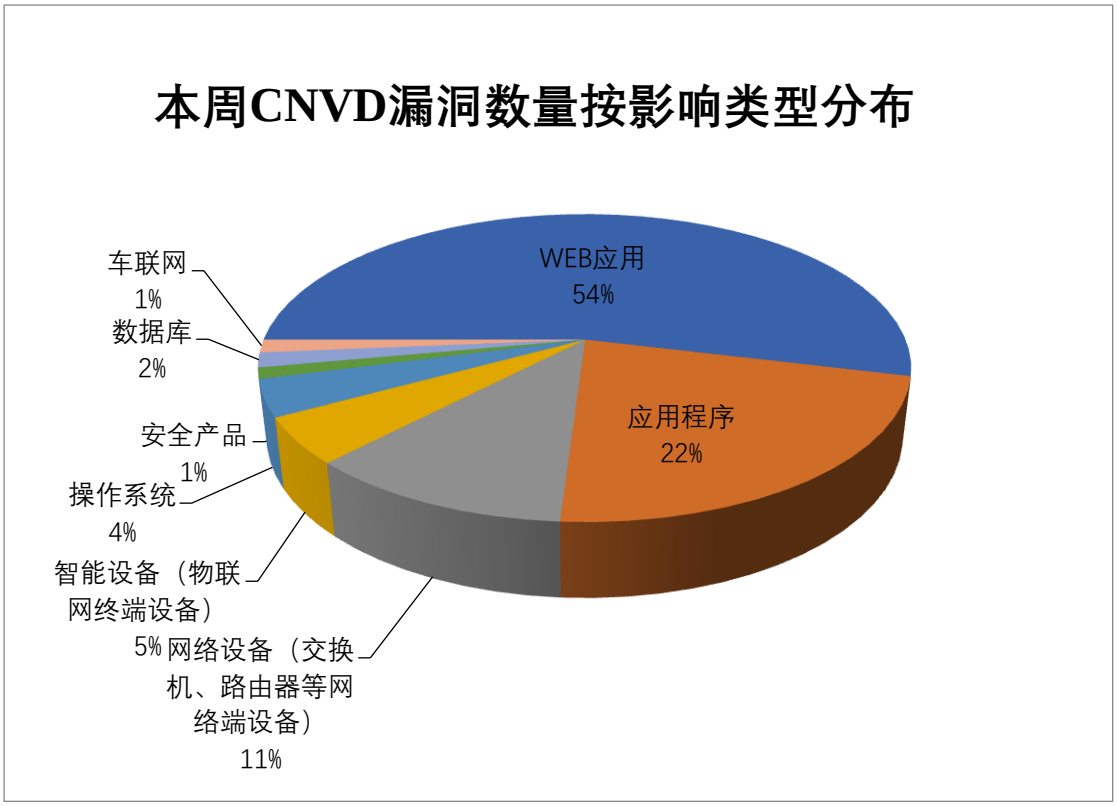

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、北京星网锐捷网络技术有限公司、OTFCC 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	用友网络科技股份有限公司	42	8%
2	北京星网锐捷网络技术有限公司	22	4%

3	OTFCC	20	4%
4	Google	18	4%
5	Microsoft	12	2%
6	IBM	11	2%
7	Linux	10	2%
8	北京百卓网络技术有限公司	9	2%
9	比亚迪股份有限公司	7	1%
10	其他	366	71%

本周行业漏洞收录情况

本周，CNVD 收录了 45 个电信行业漏洞，38 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Advantech WebAccess 信息泄露漏洞（CNVD-2024-07863）、Google Android 权限提升漏洞（CNVD-2024-07857）”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/

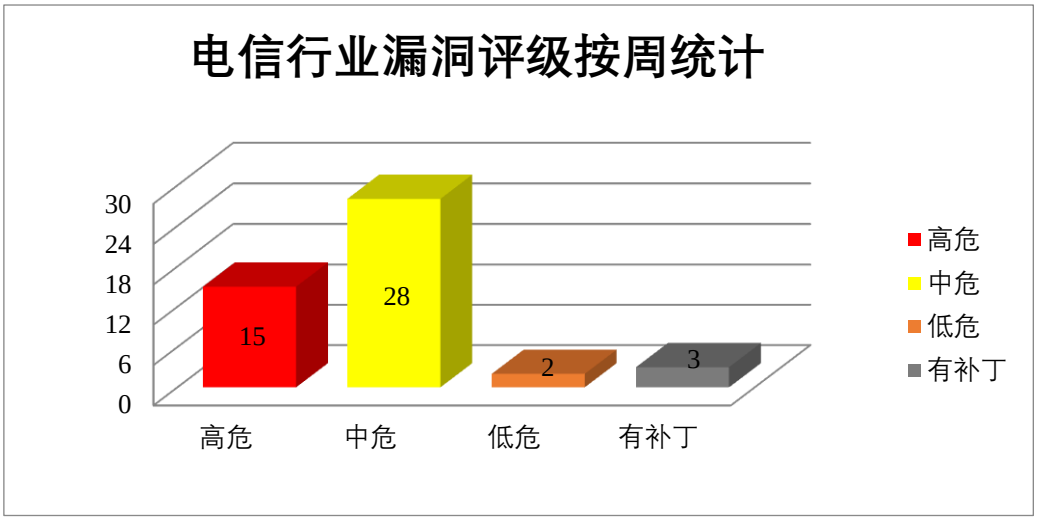

图 3 电信行业漏洞统计

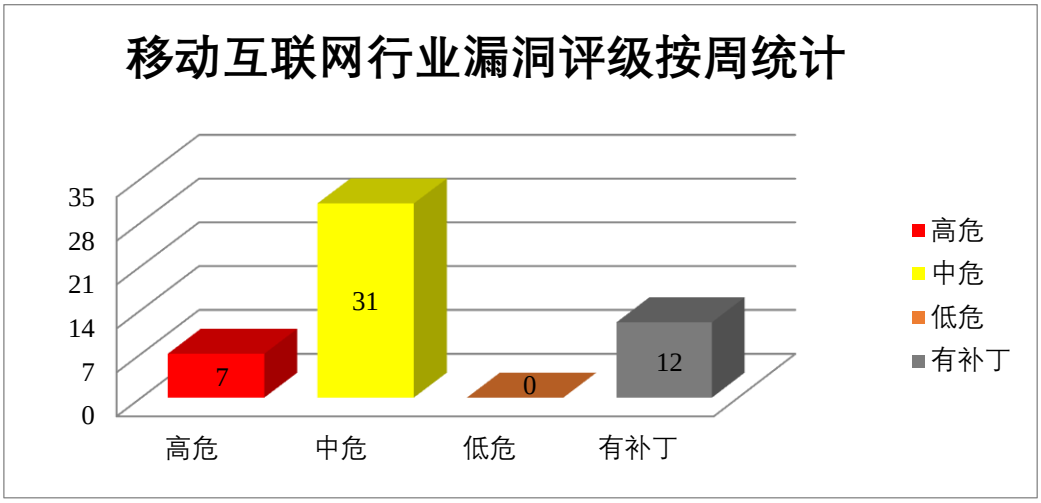

图 4 移动互联网行业漏洞统计

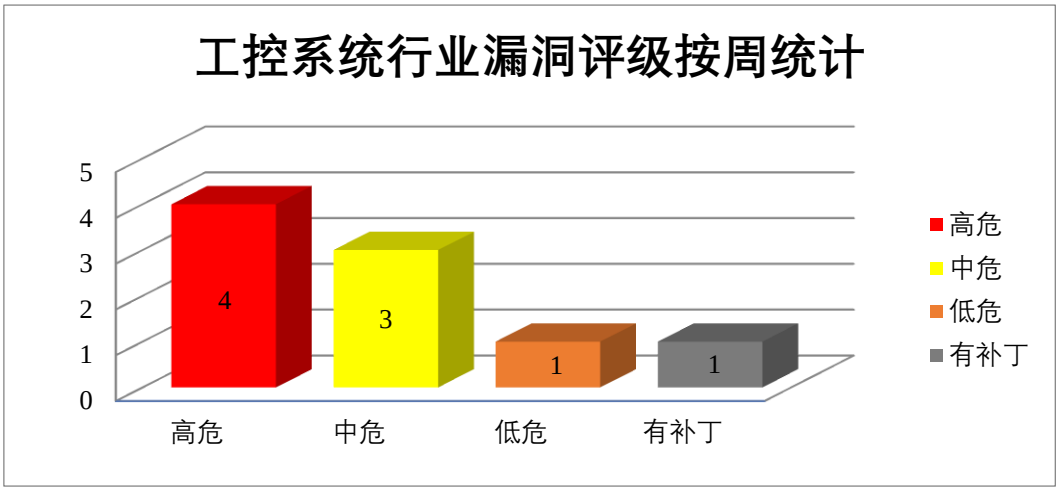

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Tivoli Application Dependency Discovery Manager（TADDM）是美国国际商业机器（IBM）公司的一套 IT 服务管理解决方案中的产品。该产品提供了健全的自动化应用程序映射和发现，帮助管理员了解业务应用程序的结构、状态、配置和变更历史记录。IBM Security Access Manager 是一款应用于信息安全管理的产品。该产品通过面向 Web、移动和云计算的集成设备来实现访问管理控制。IBM Cloud Pak System 是一套具有可配置、预集成软件的全栈、融合基础架构。该产品支持跨混合云部署、管理和移动应用程序环境。IBM Tivoli Application Dependency Discovery Manager（TADDM）是一套 IT 服务管理解决方案中的产品。该产品提供了健全的自动化应用程序映射和发现，帮助管理员了解业务应用程序的结构、状态、配置和变更历史记录。IBM Security Verify Access（ISAM）是一款提高用户访问安全的服务。该服务通过使用基于风

险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。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，消耗内存资源，提升权限等。

CNVD 收录的相关漏洞包括：IBM Tivoli Application Dependency Discovery Manager 权限提升漏洞、IBM Security Access Manager 未授权访问漏洞、IBM Cloud Pak System 信息泄露漏洞（CNVD-2024-07607）、IBM Tivoli Application Dependency Discovery Manager HTTP 头部注入漏洞、IBM Security Verify Access 权限提升漏洞、IBM Security Verify Access 拒绝服务漏洞、IBM Security Access Manager 数据伪造问题漏洞、IBM Security Access Manager XML 外部实体注入漏洞。其中，“IBM Security Access Manager 未授权访问漏洞、IBM Cloud Pak System 信息泄露漏洞（CNVD-2024-07607）、IBM Tivoli Application Dependency Discovery Manager HTTP 头部注入漏洞、IBM Security Access Manager XML 外部实体注入漏洞”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-2024-07603
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07609
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07607
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07606
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07613
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07612
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07611
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07610

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，在系统上执行任意代码，获得提升的特权等。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2024-07840）、Google Chrome Canvas 模块内存错误引用漏洞、Google Chrome Network 模块内存错误引用漏洞、Google Chrome WebRTC 模块内存错误引用漏洞、Google Chrome Reading Mode 模块内存错误引用漏洞、Google Chrome Passwords 模块内存错误引用漏洞、Google Chrome Web Audio 模块内存错误引用漏洞、Google Android 权限提升漏洞（CNVD-2024-07854）。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-2024-07840
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07841

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07842

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07844

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07845

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07846

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07847

https://www.cnvd.org.cn/flaw/show/CNVD-2024-07854

3、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 cgroup blkio 内存泄漏，系统崩溃，提升权限等。

CNVD 收录的相关漏洞包括：Linux Kernel 资源管理错误漏洞（CNVD-2024-08096、CNVD-2024-08091、CNVD-2024-08094、CNVD-2024-08093）、Linux kernel 拒绝服务漏洞（CNVD-2024-08090）、Linux kernel 代码问题漏洞（CNVD-2024-08095、CNVD-2024-08087）、Linux Kernel ksmbd SMB2_SESSION_SETUP 拒绝服务漏洞。其中，“Linux Kernel ksmbd SMB2_SESSION_SETUP 拒绝服务漏洞”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-2024-08087

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08091

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08090

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08095

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08094

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08093

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08097

https://www.cnvd.org.cn/flaw/show/CNVD-2024-08096

4、Microsoft 产品安全漏洞

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。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，在系统上获得提升的权限等。

CNVD 收录的相关漏洞包括：Microsoft Edge for Android 欺骗漏洞、Microsoft Edge for Android 信息泄露漏洞、Microsoft Edge (Chromium-based)安全绕过漏洞、Microsoft Edge (Chromium-based)信息泄露漏洞（CNVD-2024-07804、CNVD-2024-07803）、Microsoft Edge (Chromium-based)权限提升漏洞（CNVD-2024-07816、CNVD-2024-07817、CNVD-2024-07793）。其中，“Microsoft Edge (Chromium-based)安全绕过漏洞、Microsoft Edge (Chromium-based)权限提升漏洞（CNVD-2024-07816、CNVD-2024-078

17）”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-2024-07793
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07799
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07797
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07800
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07804
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07803
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07816
https://www.cnvd.org.cn/flaw/show/CNVD-2024-07817

5、TOTOLINK EX1800T lanIp 参数命令执行漏洞

TOTOLINK EX1800T 是中国吉翁电子（TOTOLINK）公司的一款 Wi-Fi 范围扩展器。本周，TOTOLINK EX1800T 被披露存在命令执行漏洞。攻击者可利用此漏洞在系统上执行任意命令。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-2024-07858

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-2024-07609	IBM Security Access Manager 未授权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7106586
CNVD-2024-07607	IBM Cloud Pak System 信息泄露漏洞（CNVD-2024-07607）	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/7105357
CNVD-2024-07800	Microsoft Edge (Chromium-based)安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20675
CNVD-2024-07840	Google Chrome 安全绕过漏洞（CNVD-2024-07840）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
CNVD-2024	Google Android Framework		厂商已发布了漏洞修复程序，请及

-07855	权限提升漏洞（CNVD-2024-07855）		时关注更新：https://source.android.com/docs/security/bulletin/2023-07-01?hl=zh-cn
CNVD-2024-07856	Google Android Framework 权限提升漏洞（CNVD-2024-07856）		厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/2023-07-01?hl=zh-cn
CNVD-2024-07862	Advantech R-SeeNet 信息泄露漏洞		用户可参考如下厂商提供的安全补丁以修复该漏洞：https://icr.advantech.cz/products/software/r-seenet
CNVD-2024-07867	WordPress 插件 BA Plus 跨站脚本漏洞		厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/ba-plus-before-after-image-slider-free/
CNVD-2024-08088	Apache InLong 代码问题漏洞（CNVD-2024-08088）		目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://github.com/apache/inlong/pull/9331
CNVD-2024-08097	Linux Kernel ksmbd SMB2_SESSION_SETUP 拒绝服务漏洞		用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/torvalds/linux/commit/ea174a91893956450510945a0c5d1a10b5323656

小结：本周，IBM 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，消耗内存资源，提升权限等。此外，Google、Linux、Microsoft 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，获取敏感信息，在系统上执行任意代码，获得提升的特权等。另外，TOTOLINK EX1800T 被披露存在命令执行漏洞。攻击者可利用此漏洞在系统上执行任意命令。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、Yifan YF325 gozila_cgi 函数缓冲区溢出漏洞

验证描述

Yifan YF325 是一款工业蜂窝路由器。

Yifan YF325 gozila_cgi 函数存在缓冲区溢出漏洞，该漏洞源于 gozila_cgi 函数中的 next_page 参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://talosintelligence.com/vulnerability_reports/TALOS-2023-1761

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-07860

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. ESET 修复了 Windows 产品中的本地权限提升漏洞

Securityaffairs 网站消息，网络安全公司 ESET 已经解决了其 Windows 安全方案中的一个权限提升漏洞。

参考链接：https://www.freebuf.com/news/391969.html

2. SolarWinds 曝出五个 RCE 漏洞

SolarWinds 近期修补了 Access Rights Manager (ARM)解决方案中的五个远程代码执行 RCE 漏洞，其中包括三个允许未验证利用的安全漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/solarwinds-fixes-critical-rce-bugs-in-access-rights-audit-solution/

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