国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 01 月 01 日-2024 年 01 月 07 日 **2024 年第 1 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 381 个，其中高危漏洞 153 个、中危漏洞 209 个、低危漏洞 19 个。漏洞平均分值为 6.18。本周收录的漏洞中，涉及 0day 漏洞 315 个（占 83%），其中互联网上出现“Dreamer CMS 跨站请求伪造漏洞（CNVD-2024-00216）、JFinalCMS 跨站脚本漏洞（CNVD-2024-00217）”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 5215 个，与上周（109390 个）环比减少 95%。

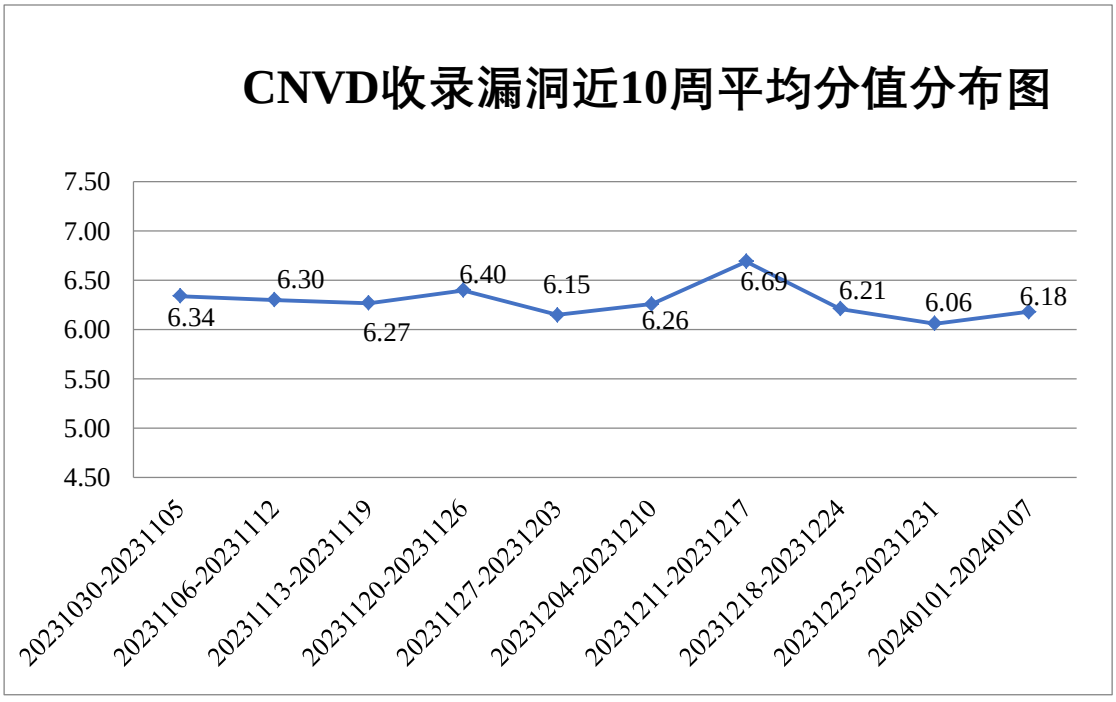

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 起，向基础电

信企业通报漏洞事件 1 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 346 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 73 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 27 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：

中興保全科技股份有限公司、中兴通讯股份有限公司、中孚信息股份有限公司、智互联（深圳）科技有限公司、支付宝（中国）网络技术有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、长沙亿拓传感科技有限公司、长沙砼软信息科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、英万齐软件技术（北京）有限公司、熊猫智慧水务有限公司、新能康技术有限公司、西安交大捷普网络科技有限公司、西安得买啦网络科技有限公司、武汉玖玖珈网络科技有限公司、无锡信捷电气股份有限公司、网是科技股份有限公司、网神信息技术（北京）股份有限公司、网强信息技术（上海）有限公司、推想医疗科技股份有限公司、通州区华丽软件工作室、天维尔信息科技股份有限公司、天津安捷物联科技股份有限公司、台达电子企业管理（上海）有限公司、随锐科技集团股份有限公司、速达软件技术（广州）有限公司、苏州中来光伏新材股份有限公司、深圳希施玛数据科技有限公司、深圳市粤豪珠宝有限公司、深圳市赢家服饰有限公司、深圳市企企通科技有限公司、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、深圳市吉祥腾达科技有限公司、深圳市道尔智控科技股份有限公司、上海卓卓网络科技有限公司、上海七慧网络科技有限公司、上海蓝矩信息科技有限公司、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、上海布雷德科技有限公司、山东卓文信息科技有限公司、山东科德电子有限公司、厦门四信通信科技有限公司、厦门极风网络科技有限公司、润申信息科技（上海）有限公司、锐捷网络股份有限公司、奇瑞汽车股份有限公司、普联技术有限公司、乐金电子（中国）有限公司、蓝网科技股份有限公司、京瓷办公信息系统（中国）有限公司、金蝶软件（中国）有限公司、捷并思（上海）信息技术有限责任公司、江苏天瑞仪器股份有限公司、江苏景枫投资控股集团有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南听风者信息科技有限公司、湖北心拓心理健康科技有限公司、宏脉信息技术（广州）股份有限公司、恒锋信息科技股份有限公司、河南易税科技有限公司、杭州海康威视数字技术股份有限公司、杭州奥能电源设备有限公司、杭州安恒信息技术股份有限公司、广州市天翎网络科技有限公司、广州市乐天科技有限公司、广州市保伦电子有限公司、广州安普达电子技术有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、富士施乐（中国）有限公司、福州网钛软件科技有限公司、福建科立讯通信有限公司、飞哥立桩（北京）新能源科技有限公司、东软教育科技集团有限公司、东方希望集团有限公司、帝国软件、成都卓越远扬信息技术有限公司、成都四相致新科技有

限公司、成都华栖云科技有限公司、北京中长石基信息技术股份有限公司、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、北京星网锐捷网络技术有限公司、北京信达网安科技有限公司、北京通达信科科技有限公司、北京数码视讯科技股份有限公司、北京世纪超星信息技术发展有限责任公司、北京润乾信息系统技术有限公司、北京瑞星网安技术股份有限公司、北京清大新洋科技有限公司、北京巧巧时代网络科技有限公司、北京金和网络股份有限公司、北京海文互知网络技术有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、北大医疗信息技术有限公司、安美世纪（北京）科技有限公司、爱普生（中国）有限公司、zzcms 和 WAVLINK。

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、新华三技术有限公司、北京数字观星科技有限公司、深信服科技股份有限公司、北京神州绿盟科技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、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、快页信息技术有限公司、湖南泛联新安信息科技有限公司、安徽天行网安信息安全技术有限公司、贵州多彩网安科技有限公司、江苏云天网络安全技术有限公司、上海直画科技有限公司、中孚安全技术有限公司、博智安全科技股份有限公司、南京先维信息技术有限公司、亚信科技（成都）有限公司、北京冠程科技有限公司、西藏熙安信息技术有限责任公司、安徽锋刃信息科技有限公司、深圳昂楷科技有限公司、交通运输信息安全中心有限公司、江苏晟晖信息科技有限公司、上海谋乐网络科技有限公司、北京山石网科信息技术有限公司、河南悦海数安科技有限公司、江苏百达智慧网络科技有限公司、江苏极元信息技术有限公司、国网山东省电力公司、贵州华黔信安信息技术有限公司、合肥梆梆信息科技有限公司、济南时代确信信息安全测评有限公司、北京中关村实验室、建信金融科技有限责任公司、北京天下信安技术有限公司、任子行网络技术股份有限公司、北京卓识网安技术股份有限公司、国网上海市电力公司、杭州默安科技有限公司、杭州智顺科技有限公司、广西网信信息技术有限公司、苏州棱镜七彩信息科技有限公司、山东旭正信息科技有限公司及其他个人白帽子向 CNVD 提交了 5215 个以事件型漏洞为主的原创漏洞，其中包括上海交大、奇安信网神（补天平台）、斗象科技（漏洞盒子）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 3187 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
上海交大	1122	1122
奇安信网神（补天平台）	1110	1110

北京启明星辰信息安全技术有限公司	603	15
斗象科技（漏洞盒子）	484	484
三六零数字安全科技集团有限公司	471	471
新华三技术有限公司	387	0
北京数字观星科技有限公司	305	0
深信服科技股份有限公司	157	0
北京神州绿盟科技有限公司	119	0
杭州安恒信息技术股份有限公司	80	2
安天科技集团股份有限公司	52	0
中国电信集团系统集成有限责任公司	32	0
北京天融信网络安全技术有限公司	25	25
北京长亭科技有限公司	22	0
杭州迪普科技股份有限公司	10	0
阿里云计算有限公司	8	8
北京安信天行科技有限公司	6	6
京东科技信息技术有限公司	4	4
长春嘉诚信息技术股份有限公司	2	2
华为技术有限公司	1	1
北京智游网安科技有限公司	1	1
西安四叶草信息技术	1	1

有限公司		
江苏金盾检测技术股份有限公司	91	91
河南东方云盾信息技术有限公司	48	48
内蒙古洞明科技有限公司	34	34
快页信息技术有限公司	26	26
湖南泛联新安信息科技有限公司	21	21
安徽天行网安信息安全技术有限公司	18	18
贵州多彩网安科技有限公司	16	16
江苏云天网络安全技术有限公司	16	16
上海直画科技有限公司	15	15
中孚安全技术有限公司	11	11
博智安全科技股份有限公司	11	11
南京先维信息技术有限公司	9	9
亚信科技（成都）有限公司	9	9
北京冠程科技有限公司	8	8
西藏熙安信息技术有限责任公司	7	7
安徽锋刃信息科技有限公司	7	7
深圳昂楷科技有限公司	6	6

交通运输信息安全中心有限公司	6	6
江苏晟晖信息科技有限公司	5	5
上海谋乐网络科技有限公司	4	4
北京山石网科信息技术有限公司	4	4
河南悦海数安科技有限公司	3	3
江苏百达智慧网络科技有限公司	3	3
江苏极元信息技术有限公司	3	3
国网山东省电力公司	2	2
贵州华黔信安信息技术有限公司	2	2
合肥梆梆信息科技有限公司	2	2
济南时代确信信息安全测评有限公司	2	2
北京中关村实验室	2	2
建信金融科技有限责任公司	2	2
北京天下信安技术有限公司	1	1
任子行网络技术股份有限公司	1	1
北京卓识网安技术股份有限公司	1	1
国网上海市电力公司	1	1
杭州默安科技有限公司	1	1
杭州智顺科技有限公司	1	1

广西网信信息技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
山东旭正信息科技有限公司	1	1
CNCERT 贵州分中心	5	5
个人	1556	1556
报送总计	6965	5215

本周漏洞按类型和厂商统计

本周，CNVD 收录了 381 个漏洞。WEB 应用 195 个，应用程序 103 个，网络设备（交换机、路由器等网络端设备）48 个，操作系统 18 个，智能设备（物联网终端设备）11 个，数据库 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	195
应用程序	103
网络设备（交换机、路由器等网络端设备）	48
操作系统	18
智能设备（物联网终端设备）	11
数据库	6

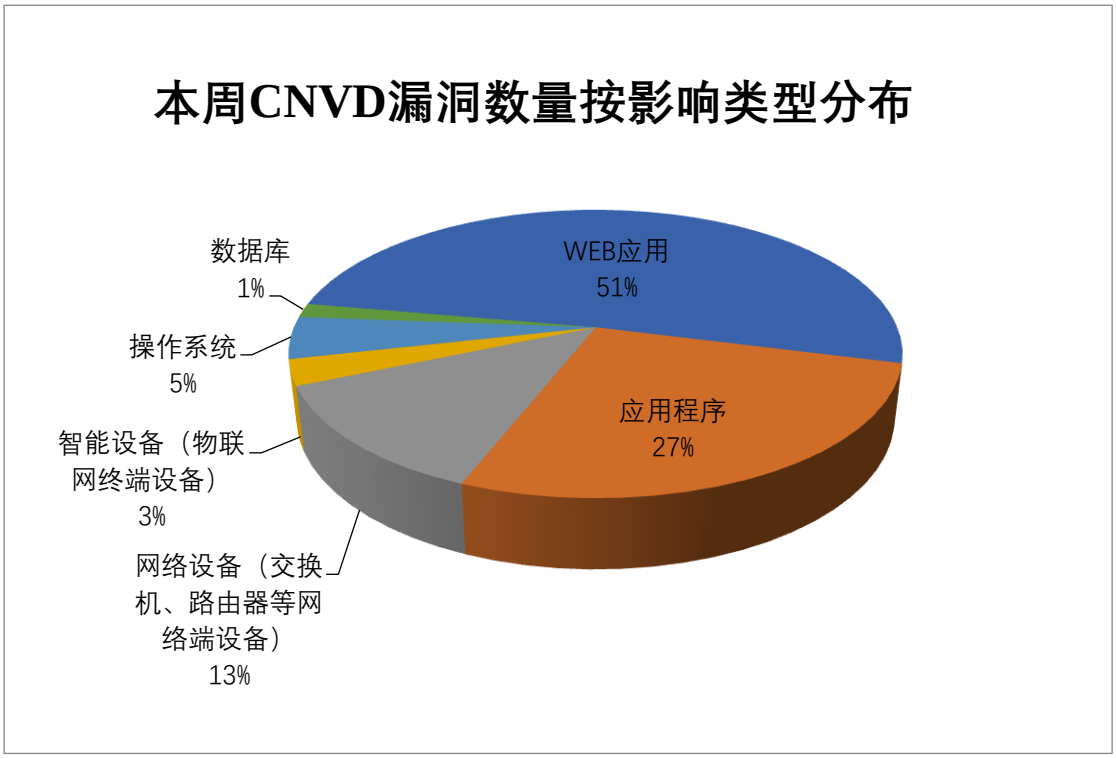

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、北京星网锐捷网络技术有限公司、DELL 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	Google	20	5%
2	北京星网锐捷网络技术有限公司	18	5%
3	DELL	10	3%
4	Microsoft	10	3%
5	北京百卓网络技术有限公司	10	3%
6	Adobe	10	3%
7	用友网络科技股份有限公司	10	2%
8	WordPress	9	2%
9	广西海豚有海信息科技有限公司	8	2%
10	其他	276	72%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，34 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，“Mitsubishi Electric MELSEC-F Series 身份验证错误漏洞”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/

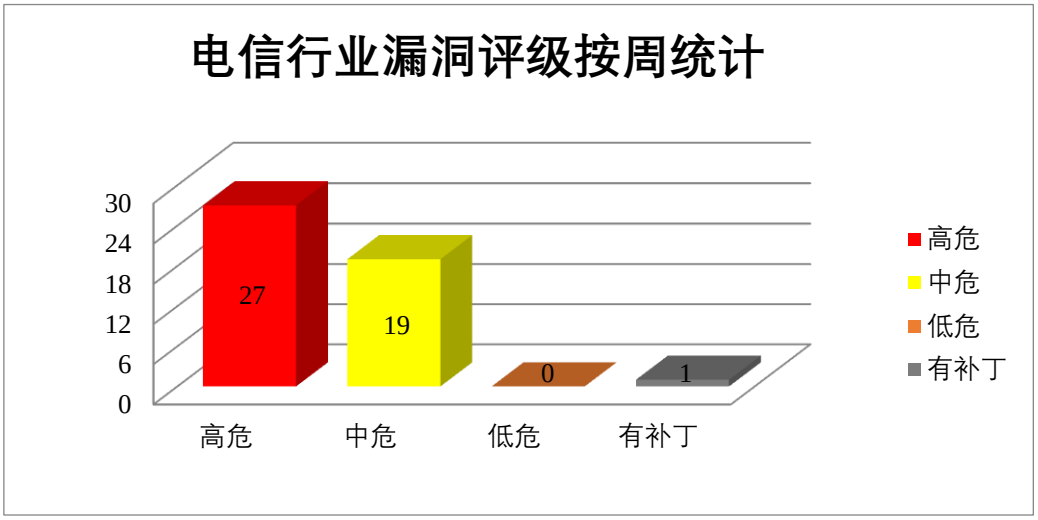

图 3 电信行业漏洞统计

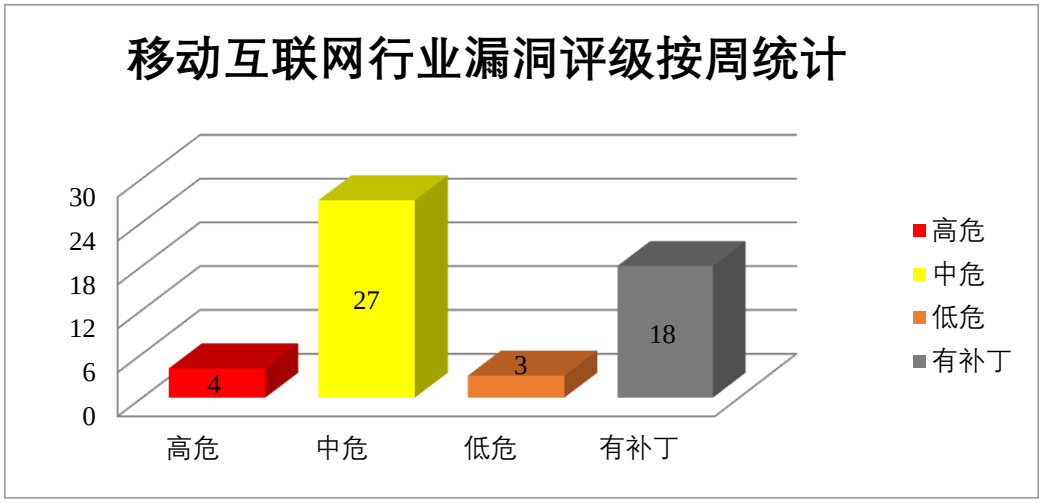

图 4 移动互联网行业漏洞统计

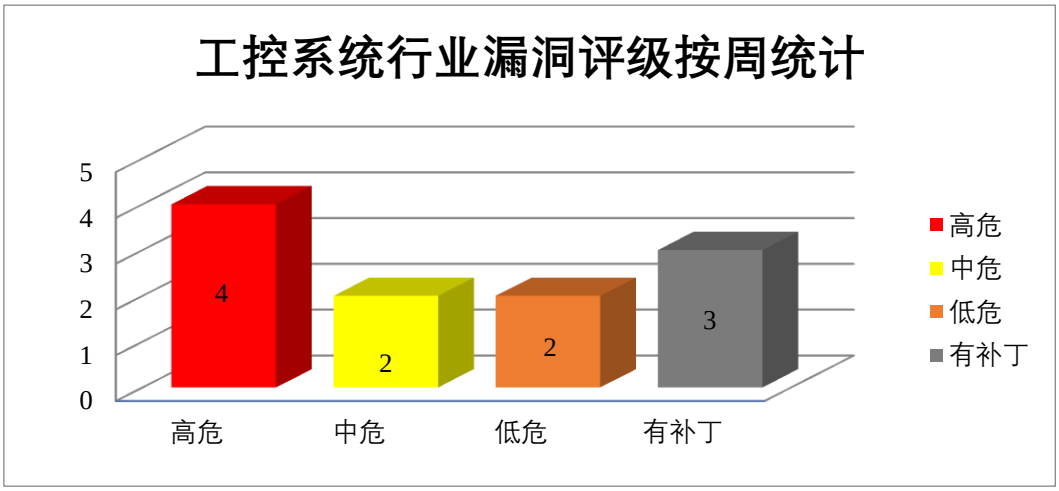

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-00337、CNVD-2024-00336、CNVD-2024-00335、CNVD-2024-00339、CNVD-2024-00338、CNVD-2024-00342、CNVD-2024-00341、CNVD-2024-00340）。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-2024-00337
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00336
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00335
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00339
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00338
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00342
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00341
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00340

2、 DELL 产品安全漏洞

Dell Virtual Appliance Manager 是美国戴尔（Dell）公司的一个虚拟设备管理器。Dell Networking OS10 是一款交换机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从目标系统读取任意文件，在受影响的系统上执行任意操作系统命令，导致网络中断等。

CNVD 收录的相关漏洞包括：Dell Virtual Appliance Manager 命令注入漏洞（CNVD-2024-00186、CNVD-2024-00189、CNVD-2024-00185、CNVD-2024-00188）、Dell Virtual Appliance Manager 任意文件读取漏洞（CNVD-2024-00187、CNVD-2024-00191）、Dell Virtual Appliance Manager 信息泄露漏洞、Dell Networking OS10 拒绝服务漏洞。其中，除“Dell Virtual Appliance Manager 任意文件读取漏洞（CNVD-2024-00187）”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-2024-00186
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00185

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00189

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00188

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00187

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00191

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00190

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00192

3、 Google 产品安全漏洞

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取敏感信息，提升权限。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2024-00159、CNVD-2024-00160、CNVD-2024-00161、CNVD-2024-00162、CNVD-2024-00163、CNVD-2024-00164、CNVD-2024-00165）、Google Android 权限提升漏洞（CNVD-2024-00665）。其中，“Google Android 权限提升漏洞（CNVD-2024-00665）”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-2024-00159

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00160

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00161

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00162

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00163

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00164

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00165

https://www.cnvd.org.cn/flaw/show/CNVD-2024-00665

4、 Microsoft 产品安全漏洞

Microsoft Dynamics 365 是美国微软（Microsoft）公司的一套适用于跨国企业的 ERP 业务解决方案。该产品包括财务管理、生产管理和商业智能管理等。Microsoft Dynamics 365 (on-premises)是一组智能商业应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行跨站脚本攻击，导致系统拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-00197、CNVD-2024-00201、CNVD-2024-00200、CNVD-2024-00199、CNVD-2024-00198、CNVD-2024-00203、CNVD-2024-00202）、Microsoft Dynamics 365 for Finance and Operations 拒绝服务漏洞。其中，除“Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-00198）”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-2024-00197
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00196
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00201
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00200
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00199
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00198
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00203
https://www.cnvd.org.cn/flaw/show/CNVD-2024-00202

5、D-Link Go-RT-AC750 命令注入漏洞

D-Link GO-RT-AC750 是中国友讯（D-Link）公司的一款无线双频简易路由器。本周，D-Link Go-RT-AC750 被披露存在命令注入漏洞。攻击者可利用该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-2024-00218

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-2024-00186	Dell Virtual Appliance Manager 命令注入漏洞（CNVD-2024-00186）	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/000220427/dsa-2023-443-dell-powermaxos-5978-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-security-update-for-multiple-vulnerabilities
CNVD-2024-00189	Dell Virtual Appliance Manager 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.dell.com/support/kbdoc/en-us/000220427/dsa-2023-443-dell-powermaxos-5978-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-security-update-for-multiple-vulnerabilitie

			s
CNVD-2024-00191	Dell Virtual Appliance Manager 任意文件读取漏洞	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/000220427/dsa-2023-443-dell-powermaxos-5978-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-security-update-for-multiple-vulnerabilities
CNVD-2024-00192	Dell Networking OS10 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://www.dell.com/support/kbdoc/en-us/000220138/dsa-2023-278-dell-networking-os10-security-updates-for-uncontrolled-resource-consumption
CNVD-2024-00195	Mozilla Firefox 信息泄露漏洞（CNVD-2024-00195）	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/firefox/121.0/releasenotes/
CNVD-2024-00197	Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-00197）	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-2023-36020
CNVD-2024-00200	Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-00200）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-38164
CNVD-2024-00203	Microsoft Dynamics 365 (on-premises)跨站脚本漏洞（CNVD-2024-00203）	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-2023-33171
CNVD-2024-00210	Mitsubishi Electric MELSEC-F Series 身份验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-012_en.pdf
CNVD-2024-00665	Google Android 权限提升漏洞（CNVD-2024-00665）	高	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/android-14

小结：本周，Adobe 产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。此外，DELL、Google、Microsoft 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，执行跨站脚本攻击，在受影响的系统上执行任意操作系统命令，导致系统拒绝服务。另外，D-Link Go-RT-AC750 被披露存在命令注入漏洞。攻击者可利用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、JFinalCMS 跨站脚本漏洞（CNVD-2024-00217）

验证描述

JFinalCMS 是一个内容管理系统。

JFinalCMS 5.0.0 版本存在跨站脚本漏洞，该漏洞源于 carousel image editing 对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/Jarvis-616/cms/blob/master/There%20is%20a%20storage%20type%20XSS%20for%20carousel%20image%20editing.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-00217

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. 谷歌 2024 年首个 Chrome 安全更新修复了 6 个漏洞

谷歌宣布了 2024 年首个 Chrome 安全更新，解决了 6 个漏洞，其中包括外部研究人员报告的 4 个漏洞。其中编号 CVE-2024-0224 是 Chrome 的 WebAudio 组件中的释放后使用缺陷。

参考链接：http://www.anquan419.com/knews/24/6512.html

2. Terrapin 漏洞影响 SSH 协议的安全性

威胁攻击者能够利用漏洞破坏安全通道的完整性，从而降低 SSH 连接的安全性。

参考链接：https://www.freebuf.com/news/388549.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