国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 09 月 16 日-2024 年 09 月 22 日 **2024 年第 38 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 253 个，其中高危漏洞 141 个、中危漏洞 108 个、低危漏洞 4 个。漏洞平均分值为 6.98。本周收录的漏洞中，涉及 0day 漏洞 186 个（占 74%），其中互联网上出现“FastCMS 跨站脚本漏洞（CNVD-2024-38571）、SeaCMS 跨站脚本漏洞（CNVD-2024-38573）”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 12328 个，与上周（28055 个）环比减少 56%。

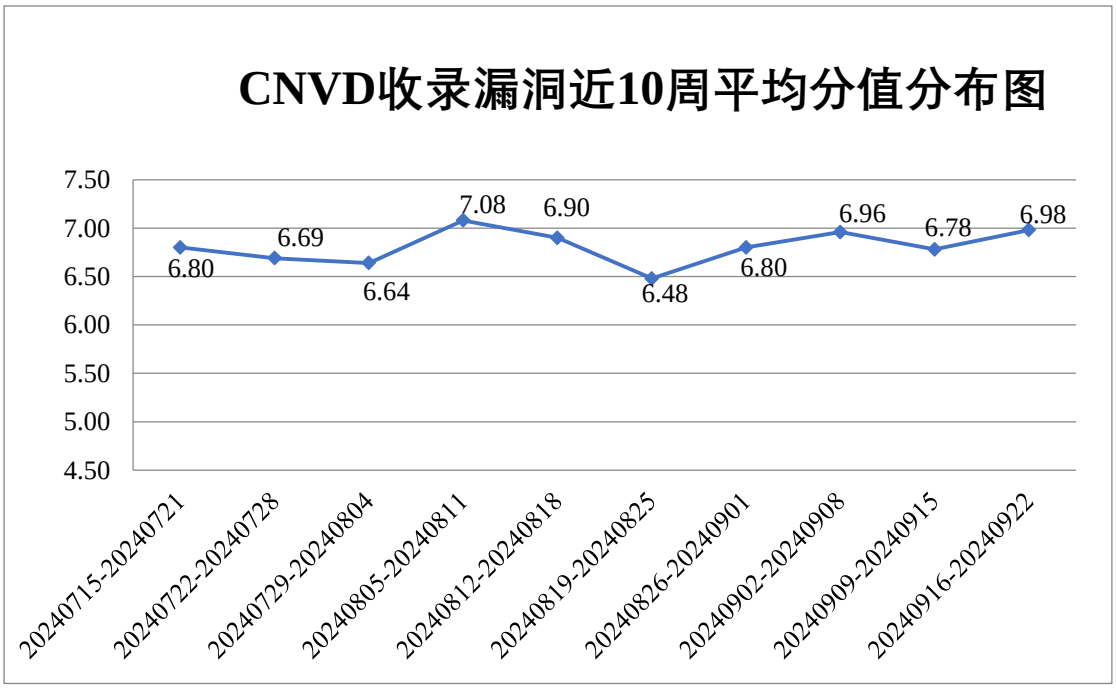

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 4 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 353 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 27 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 7 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：

紫光软件系统有限公司、重庆天知软件技术有限公司、中亿丰数字科技集团有限公司、智互联（深圳）科技有限公司、浙江大华技术股份有限公司、漳州市芗城帝兴软件开发有限公司、漳州豆壳网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新开普电子股份有限公司、西门子（中国）有限公司、武汉深之度科技有限公司、无锡信捷电气股份有限公司、网神信息技术（北京）股份有限公司、通州区华丽软件工作室、拓尔思信息技术股份有限公司、索尼（中国）有限公司、神州数码控股有限公司、深圳市天凯智能科技有限公司、深圳市磊科实业有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海甄云科技信息有限公司、上海移远通信技术股份有限公司、上海联影医疗科技股份有限公司、上海艾泰科技有限公司、山东思达特测控设备有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、青岛东胜伟业软件有限公司、麒麟软件有限公司、摩莎科技（上海）有限公司、柯尼卡美能达集团、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华平信息技术股份有限公司、恒信汽车集团股份有限公司、合肥六出网络科技有限公司、杭州映云科技有限公司、杭州品联科技有限公司、哈尔滨新中新电子股份有限公司、哈尔滨伟成科技有限公司、广州小橘灯信息科技有限公司、广州市超易信息科技有限公司、广州巨杉软件开发有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、佛山市杜特软件科技有限公司、飞利达科技股份有限公司、东华软件股份公司、东莞哲霖信息科技有限公司、成都天问互联科技有限公司、成都光大网络科技有限公司、畅捷通信息技术股份有限公司、沧州市凡诺广告传媒有限公司、北京云中融信网络科技有限公司、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、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京数字政通科技股份有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京力创瑞和电子科技有限公司、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、北京汉王智远科技有限公司、北京百卓网络技术有限公司、北京奥星贝斯科技有限公司、北京奥博威斯科技有限公司、安科瑞电气股份有限公司和 NETGEAR。

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、北京天融信网络安全技术有限公司、京东科技信息技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、江苏金盾检测技术股份有限公司、河北锐远网络科技有限公司、上海观安信息技术股份有限公司、淮安易云科技有限公司、北京翰慧投资咨询有限公司、安徽天行网安信息安全技术有限公司、北京卓识网安技术股份有限公司、成都久信信息技术股份有限公司、江苏晟晖信息科技有限公司、北京天下信安技术有限公司、中资网络信息安全科技有限公司、联想全球安全实验室及其他个人白帽子向 CNVD 提交了 12328 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 11126 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）	9442	9442
三六零数字安全科技集团有限公司	683	683
新华三技术有限公司	630	0
上海交大	622	622
深信服科技股份有限公司	603	6
奇安信网神（补天平台）	379	379
北京天融信网络安全技术有限公司	277	0
京东科技信息技术有限公司	95	0
北京启明星辰信息安全技术有限公司	70	0
杭州安恒信息技术股份有限公司	43	6
华为技术有限公司	31	1
恒安嘉新（北京）科技股份公司	22	0
远江盛邦（北京）网络安全科技股份有限	18	18

公司		
北京长亭科技有限公司	7	1
中国电信股份有限公司网络安全产品运营中心	6	6
北京安信天行科技有限公司	4	4
北京升鑫网络科技有限公司（青藤云）	3	3
北京云科安信科技有限公司	2	2
长春嘉诚信息技术股份有限公司	1	1
成都卫士通信息安全技术有限公司	171	171
河南东方云盾信息技术有限公司	20	20
快页信息技术有限公司	15	15
江苏金盾检测技术股份有限公司	6	6
河北锎远网络科技有限公司	5	5
上海观安信息技术股份有限公司	5	5
淮安易云科技有限公司	5	5
北京翰慧投资咨询有限公司	3	3
安徽天行网安信息安全技术有限公司	3	3
北京卓识网安技术股份有限公司	1	1
成都久信信息技术股	1	1

份有限公司		
江苏晟晖信息科技有限公司	1	1
北京天下信安技术有限公司	1	1
中资网络信息安全科技有限公司	1	1
联想全球安全实验室	1	1
CNCERT 宁夏分中心	17	17
CNCERT 河北分中心	5	5
个人	893	893
报送总计	14092	12328

本周漏洞按类型和厂商统计

本周，CNVD 收录了 253 个漏洞。WEB 应用 142 个，网络设备（交换机、路由器等网络端设备）44 个，应用程序 38 个，智能设备（物联网终端设备）20 个，操作系统 4 个，数据库 3 个，安全产品 2 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	142
网络设备（交换机、路由器等网络端设备）	44
应用程序	38
智能设备（物联网终端设备）	20
操作系统	4
数据库	3
安全产品	2

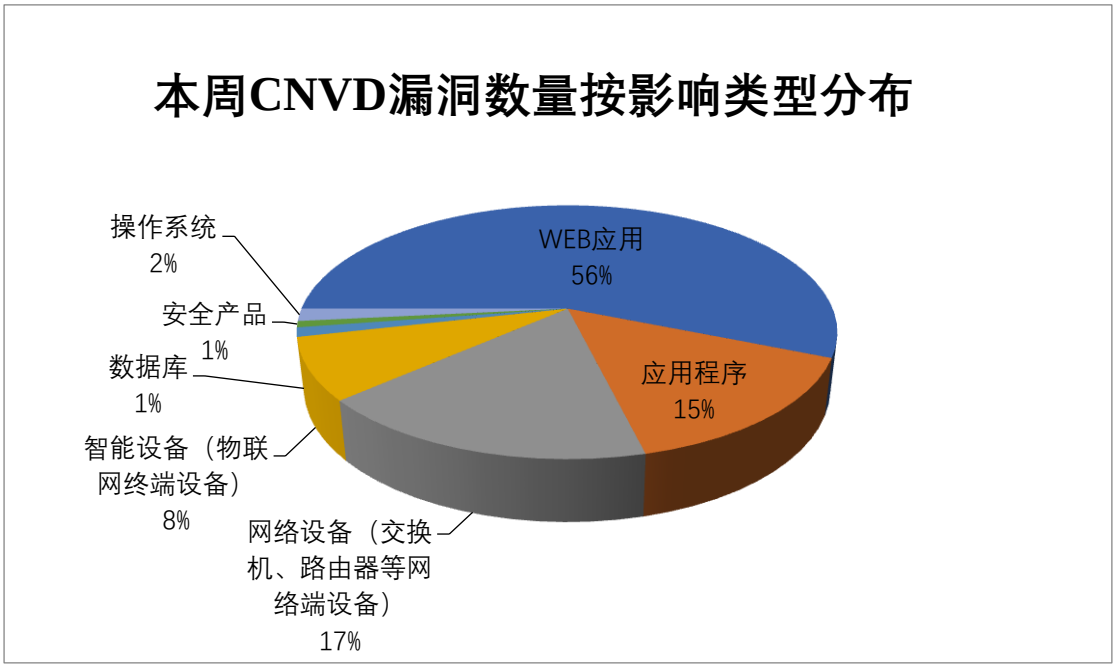

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、畅捷通信息技术股份有限公司、IBM 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	14	6%
2	畅捷通信息技术股份有限公司	11	4%
3	IBM	10	4%
4	Google	10	4%
5	Dell	8	3%
6	Adobe	8	3%
7	大连爱智控制系统有限公司	6	2%
8	杭州雄伟科技开发股份有限公司	6	2%
9	惠普贸易（上海）有限公司	5	2%
10	其他	175	70%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，8 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Tenda FH451 命令注入漏洞、Rockwell Automation

ThinManager ThinServer 输入验证错误漏洞（CNVD-2024-38545）”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/

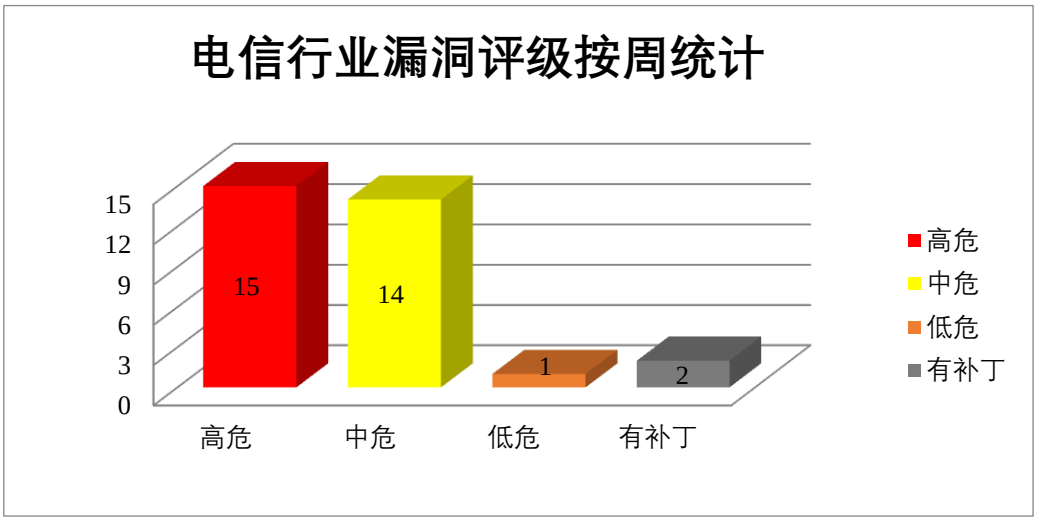

图 3 电信行业漏洞统计

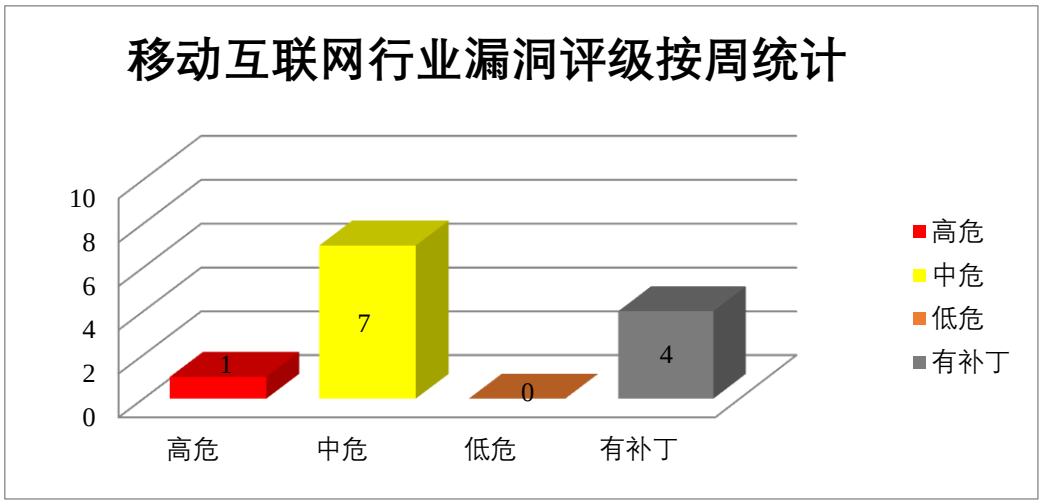

图 4 移动互联网行业漏洞统计

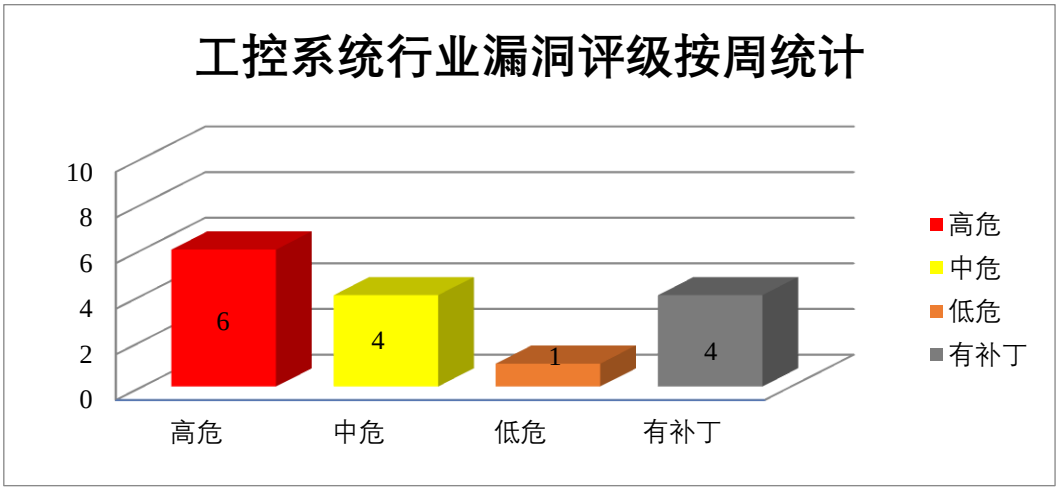

图 5 工控系统行业漏洞统计

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 InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe Acrobat Reader 是一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Illustrator 是一套基于向量的图像制作软件。Adobe Framemaker 是一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Animate 是一套 Flash 动画制作软件。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，在系统上执行任意代码，导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-38536）、Adobe InDesign 越界读取漏洞（CNVD-2024-38535）、Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-38534）、Adobe Illustrator 越界写入漏洞（CNVD-2024-38540）、Adobe Framemaker Publishing Server 信息泄露漏洞、Adobe Framemaker Publishing Server 身份验证错误漏洞（CNVD-2024-38538）、Adobe InDesign 空指针解引用漏洞（CNVD-2024-38537）、Adobe Animate 越界读取漏洞（CNVD-2024-38541）。其中，“Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-38536）、Adobe Illustrator 越界写入漏洞（CNVD-2024-38540）、Adobe Framemaker Publishing Server 信息泄露漏洞、Adobe Framemaker Publishing Server 身份验证错误漏洞（CNVD-2024-38538）”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-2024-38536

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38535

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38534

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38540

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38539

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38538

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38537

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38541

2、 Dell 产品安全漏洞

Dell BIOS 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞修改 UEFI 变量，提升系统权限，导致身份验证绕过等。

CNVD 收录的相关漏洞包括：Dell BIOS 授权问题漏洞（CNVD-2024-38332、CNVD-2024-38333）、Dell BIOS 输入验证错误漏洞（CNVD-2024-38335、CNVD-2024-38334、CNVD-2024-38338、CNVD-2024-38337、CNVD-2024-38336、CNVD-2024-38339）。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-2024-38332

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38335

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38334

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38333

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38338

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38337

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38336

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38339

3、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，使溢出缓冲区，在系统上执行任意代码或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Google Chrome Media Router 内存错误引用漏洞、Google Chrome 堆缓冲区溢出漏洞（CNVD-2024-38576、CNVD-2024-38577、CNVD-2024-38578）、Google Chrome 代码执行漏洞（CNVD-2024-38575、CNVD-2024-38581、CNVD-2024-38582）、Google Chrome 信息泄露漏洞（CNVD-2024-38583）。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-2024-38574

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38575

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38576

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38577

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38578

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38581

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38582

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38583

4、IBM 产品安全漏洞

IBM webMethods Integration 是美国国际商业机器（IBM）公司的一个混合的企业 iPaaS。IBM MQ Operator 是一种用于管理 IBM MQ 队列管理器生命周期的工具。IBM Aspera 是一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过预期的访问限制并进行资源修改，上传和执行可以在底层操作系统上执行的任意文件，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM webMethods Integration 权限提升漏洞、IBM webMethods Integration 文件上传漏洞、IBM MQ Operator 拒绝服务漏洞、IBM MQ Operator 安全绕过漏洞、IBM Aspera 信息泄露漏洞、IBM Aspera 安全绕过漏洞（CNVD-2024-38530、CNVD-2024-38533）、IBM webMethods Integration 路径遍历漏洞。其中，“IBM webMethods Integration 权限提升漏洞、IBM webMethods Integration 文件上传漏洞、IBM MQ Operator 安全绕过漏洞”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-2024-38528

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38527

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38525

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38524

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38531

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38530

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38529

https://www.cnvd.org.cn/flaw/show/CNVD-2024-38533

5、Micron Crucial MX500 Series Solid State Drives 缓冲区溢出漏洞

Micron Crucial MX500 Series Solid State Drives 是美国美光（Micron）公司的一系列固态硬盘。本周，Micron Crucial MX500 Series Solid State Drives 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞溢出缓冲区并在系统上执行任意代码。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-2024-38570

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-2024-38543	Rockwell Automation ThinManager ThinServer 输入验证错误漏洞（CNVD-2024-38543）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
CNVD-2024-38544	Rockwell Automation ThinManager ThinServer 输入验证错误漏洞（CNVD-2024-38544）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
CNVD-2024-38572	Google Chrome Autofill 内存错误引用漏洞（CNVD-2024-38572）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
CNVD-2024-38527	IBM webMethods Integration 文件上传漏洞		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/7167245
CNVD-2024-38524	IBM MQ Operator 安全绕过漏洞		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/7167732
CNVD-2024-38536	Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-38536）		厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb24-48.html
CNVD-2024-38539	Adobe Framemaker Publishing Server 信息泄露漏洞		厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html
CNVD-2024-38545	Rockwell Automation ThinManager ThinServer 输入验证错误漏洞（CNVD-2024-38545）		厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
CNVD-2024-38574	Google Chrome Media Router 内存错误引用漏洞		厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-

			desktop_10.html
CNVD-2024-38575	Google Chrome 代码执行漏洞（CNVD-2024-38575）		厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html

小结：本周，Adobe 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，在系统上执行任意代码，导致应用程序崩溃等。此外，Dell、Google、IBM 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，修改 UEFI 变量，提升系统权限，导致身份验证绕过，在系统上执行任意代码或导致应用程序崩溃等。另外，Micron Crucial MX500 Series Solid State Drives 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞溢出缓冲区并在系统上执行任意代码。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、SeaCMS 跨站脚本漏洞（CNVD-2024-38573）

验证描述

SeaCMS 是海洋 CMS（SeaCMS）公司的一套使用 PHP 编写的免费、开源的网站内容管理系统。该系统主要被设计用来管理视频点播资源。

SeaCMS 存在跨站脚本漏洞，攻击者可利用该漏洞通过注入 siteurl 参数的精心制作的有效负载执行任意 web 脚本或 HTML。

验证信息

POC 链接：https://github.com/nn0nkey/nn0nkey/blob/main/CVE-2024-44920.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-38573

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. CISA 警告 Apache HugeGraph-Server 漏洞被积极利用

美国网络安全和基础设施局（CISA）已在其已知利用漏洞（KEV）目录中添加了五个缺陷，其中包括影响 Apache HugeGraph-Server 的远程代码执行缺陷。

参考链接：https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-apache-hugegraph-server-bug/

2. 谷歌云被曝安全漏洞，或影响数百万台服务器

9 月 16 日，美国网络安全公司 Tenable 的研究人员发文称，其发现了名为“CloudImposer”的远程代码执行(RCE)漏洞，攻击者可能利用该漏洞劫持影响 GCP 的内部软件依赖项。

参考链接：https://www.secrss.com/articles/70349

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