# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2022 年 01 月 17 日-2022 年 01 月 23 日** **2022 年第 3 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 607 个，其中高危漏洞 186 个、中危漏洞 367 个、低危漏洞 54 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 282 个（占 46%），其中互联网上出现“SeedDMS 跨站脚本漏洞（CNVD-2022-05448）、Auerswald COMpact 5500R 权限提升漏洞”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事件型漏洞总数 5941 个，与上周（33637 个）环比减少 82%。

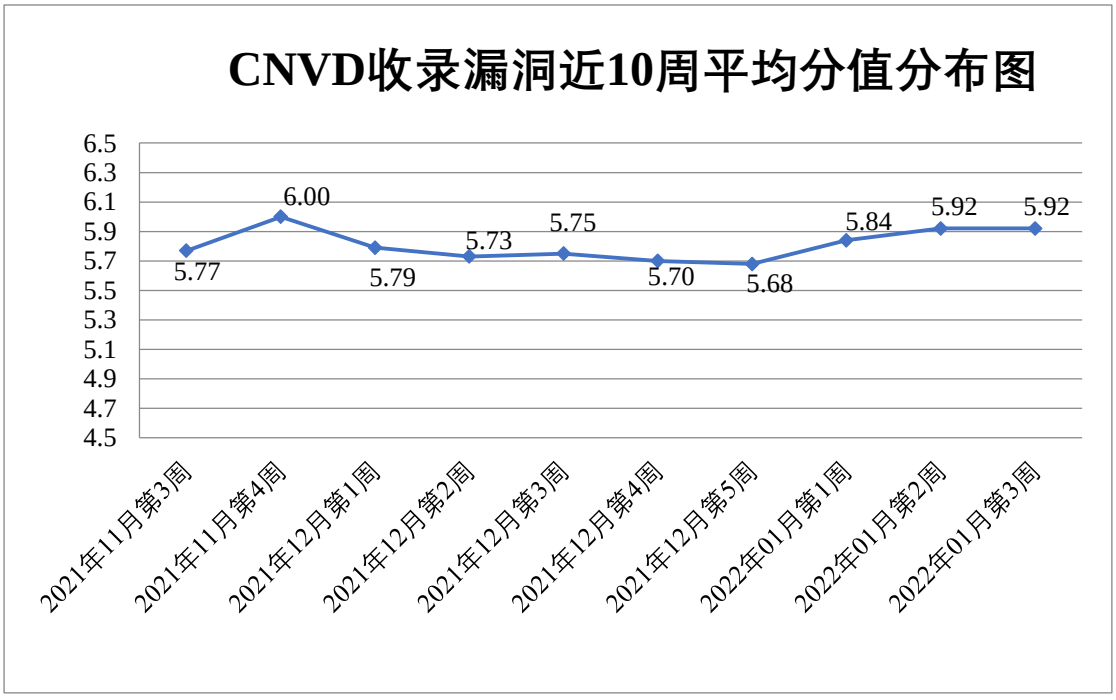


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 39 起，向基础电

信企业通报漏洞事件 35 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 605 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 87 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 108 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：

淄博闪灵网络科技有限公司、重庆中联信息产业有限责任公司、正方软件股份有限公司、浙江兰德纵横网络技术股份有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、营口爱思达计算机信息网络有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、西安艾润物联网技术服务有限责任公司、武汉富思特创新信息技术有限公司、微软（中国）有限公司、网强信息技术（上海）有限公司、天闻数媒科技（北京）有限公司、天津神州浩天科技有限公司、索尼（中国）有限公司、宿迁鑫潮信息技术有限公司、苏州思迪信息技术有限公司、苏州科达科技股份有限公司、搜狗科技发展有限公司、四川享宇科技有限公司、沈阳点动科技有限公司、深圳致软信息技术有限公司、深圳市中科网威科技有限公司、深圳市芯睿视科技有限公司、深圳市万网博通科技有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、深圳警翼智能科技股份有限公司、深圳鼎信通达股份有限公司、上海云翌通信科技有限公司、上海嵩恒网络科技股份有限公司、上海上汽安悦充电科技有限公司、上海商派网络科技有限公司、上海盘隆科技有限公司、上海南燕信息技术有限公司、上海开始网络科技有限公司、上海汉得信息技术股份有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、山东合联互联网科技有限公司、厦门凤凰创壹软件有限公司、任子行网络技术股份有限公司、人民交通出版社股份有限公司、青岛海尔生物医疗股份有限公司、青岛东胜伟业软件有限公司、青岛东胜伟业软件科技有限公司、普联技术有限公司、农夫山泉股份有限公司、宁波市科技园区明天医网科技有限公司、南宁旭东网络科技有限公司、南京科远智慧科技集团股份有限公司、联想（北京）有限公司、廊坊市极致网络科技有限公司、江西铭软科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、湖南建研信息技术股份有限公司、洪湖尔创网联信息技术有限公司、衡水金航计算机科技有限公司、河南联旺实业有限公司、河北南昊高新技术开发有限公司、和美酒店管理（上海）有限公司、合肥彼岸互联信息技术有限公司、杭州易软共创网络科技有限公司、杭州图特信息科技有限公司、杭州恩软信息技术有限公司、杭州迪普科技股份有限公司、海南赞赞网络科技有限公司、贵州觅新科技有限公司、广州红帆科技有限公司、谷歌公司、富士胶片商业创新（中国）有限公司、福建环宇通信息科技股份公司、佛山市杜特软件科技有限公司、东华医为科技有限公司、东莞市光速网络技术有限公司、大唐电信科技股份有限公司、大庆紫金桥软件技术有限公司、成都飞鱼星

科技股份有限公司、畅捷通信息技术股份有限公司、标志（中国）有限公司、北京中成科信科技发展有限公司、北京亦心科技有限公司、北京亚控科技发展有限公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京万户网络技术有限公司、北京搜狗信息服务有限公司、北京升鑫网络科技有限公司、北京山石网科信息技术有限公司、北京奇虎科技有限公司、北京良精志诚科技有限责任公司、北京华夏创新科技有限公司、北京海狸先生网络科技有限公司、北京国通创安报警网络技术有限公司、北京国炬信息技术有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、安徽阳光心健科技发展有限公司、安徽省科大奥锐科技有限公司、京瓷集团、百家 CMS 微商城、站帮主 CMS、信呼、梦想 CMS、狂雨小说 cms、好推手、zzzcms、ZZCMS、Yamaha Corporation、TaoCMS、SEMCMS、Sapido Technology Inc、Oki Electric Industry Co、MuYuCMS、Moxa、Glyph & Cog, LLC、fronius、flexwatch 和 CatFishCMS。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、新华三技术有限公司、安天科技集团股份有限公司、厦门服云信息科技有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。山东泽鹿安全技术有限公司、南京树安信息技术有限公司、内蒙古洞明科技有限公司、北京山石网科信息技术有限公司、杭州默安科技有限公司、亚信科技（成都）有限公司、河南灵创电子科技有限公司、广东蓝爵网络安全技术股份有限公司、快页信息技术有限公司、重庆都会信息科技有限公司、河南信安世纪科技有限公司、广州百蕴启辰科技有限公司、山东云天安全技术有限公司、贵州多彩宝互联网服务有限公司、福建省海峡信息技术有限公司、上海纽盾科技股份有限公司、北京远禾科技有限公司、深圳昂楷科技有限公司、海南神州希望网路有限公司、思而听网络科技有限公司、四川哨兵信息科技有限公司、联想集团、山石网科通信技术股份有限公司、浙江木链物联网科技有限公司、博智安全科技股份有限公司、杭州美创科技有限公司、中通服和信科技有限公司、有度网络安全技术有限公司、北京机沃科技有限公司、北京惠而特科技有限公司及其他个人白帽子向 CNVD 提交了 5941 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）、上海交大向 CNVD 共享的白帽子报送的 4017 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） | 2005 | 2005 |
| 奇安信网神（补天平台） | 1382 | 1382 |

| | | |
|---|---|---|
| 上海交大 | 630 | 630 |
| 北京天融信网络安全技术有限公司 | 226 | 76 |
| 新华三技术有限公司 | 226 | 0 |
| 安天科技集团股份有限公司 | 211 | 0 |
| 厦门服云信息科技有限公司 | 179 | 0 |
| 恒安嘉新（北京）科技股份公司 | 117 | 0 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 98 | 98 |
| 杭州安恒信息技术股份有限公司 | 85 | 20 |
| 北京数字观星科技有限公司 | 73 | 0 |
| 北京神州绿盟科技有限公司 | 73 | 12 |
| 天津市国瑞数码安全系统股份有限公司 | 59 | 0 |
| 西安四叶草信息技术有限公司 | 58 | 58 |
| 北京启明星辰信息安全技术有限公司 | 55 | 2 |
| 京东科技信息技术有限公司 | 20 | 20 |
| 中国电信集团系统集成有限责任公司 | 10 | 0 |
| 南京联成科技发展股份有限公司 | 9 | 9 |
| 内蒙古云科数据服务股份有限公司 | 7 | 7 |
| 南京众智维信息科技有限公司 | 6 | 6 |

| | | |
|---|---|---|
| 北京知道创宇信息技术股份有限公司 | 3 | 0 |
| 北京智游网安科技有限公司 | 1 | 1 |
| 山东泽鹿安全技术有限公司 | 177 | 177 |
| 北京华顺信安科技有限公司 | 107 | 0 |
| 南京树安信息技术有限公司 | 53 | 53 |
| 内蒙古洞明科技有限公司 | 43 | 43 |
| 北京山石网科信息技术有限公司 | 42 | 42 |
| 杭州默安科技有限公司 | 37 | 37 |
| 亚信科技（成都）有限公司 | 29 | 15 |
| 杭州迪普科技股份有限公司 | 29 | 0 |
| F5 | 25 | 0 |
| 河南灵创电子科技有限公司 | 18 | 18 |
| 广东蓝爵网络安全技术股份有限公司 | 16 | 16 |
| 快页信息技术有限公司 | 16 | 16 |
| 重庆都会信息科技有限公司 | 16 | 16 |
| 河南信安世纪科技有限公司 | 16 | 16 |
| 广州百蕴启辰科技有限公司 | 12 | 12 |
| 山东云天安全技术有限公司 | 8 | 8 |

| | | |
|---|---|---|
| 贵州多彩宝互联网服务有限公司 | 7 | 7 |
| 福建省海峡信息技术有限公司 | 4 | 4 |
| 上海纽盾科技股份有限公司 | 3 | 3 |
| 北京远禾科技有限公司 | 2 | 2 |
| 深圳昂楷科技有限公司 | 2 | 2 |
| 海南神州希望网路有限公司 | 2 | 2 |
| 思而听网络科技有限公司 | 2 | 2 |
| 四川哨兵信息科技有限公司 | 2 | 2 |
| 联想集团 | 1 | 1 |
| 山石网科通信技术股份有限公司 | 1 | 1 |
| 浙江木链物联网科技有限公司 | 1 | 1 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 杭州美创科技有限公司 | 1 | 1 |
| 中通服和信科技有限公司 | 1 | 1 |
| 有度网络安全技术有限公司 | 1 | 1 |
| 北京机沃科技有限公司 | 1 | 1 |
| 北京惠而特科技有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 1 | 1 |
| 个人 | 1112 | 1112 |

| | | |
|---|---|---|
| 报送总计 | 7323 | 5941 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 607 个漏洞。应用程序 253 个，WEB 应用 217 个，网络设备（交换机、路由器等网络端设备）68 个，智能设备（物联网终端设备）31 个，操作系统 23 个，安全产品 13 个，数据库 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 |
|---|---|
| 应用程序 | 253 |
| WEB 应用 | 217 |
| 网络设备（交换机、路由器等网络端设备） | 68 |
| 智能设备（物联网终端设备） | 31 |
| 操作系统 | 23 |
| 安全产品 | 13 |
| 数据库 | 2 |

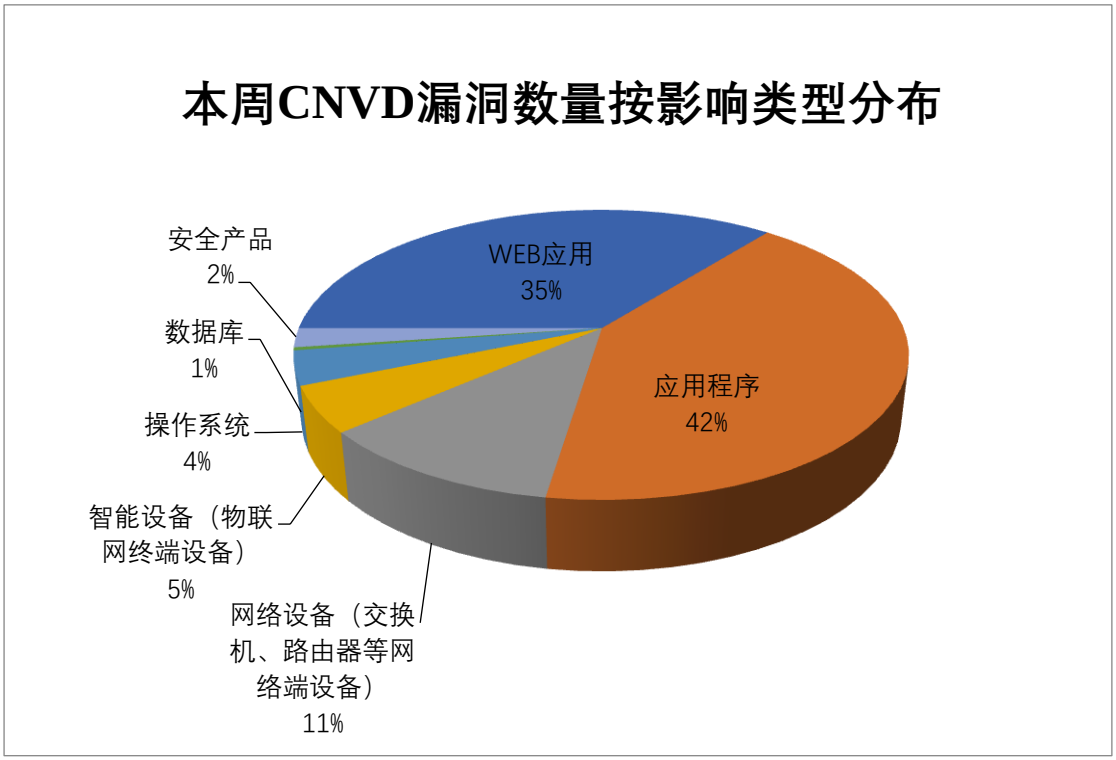


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、GPAC、Adobe 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 | IBM | 34 | 6% |
| 2 | GPAC | 31 | 5% |
| 3 | Adobe | 24 | 4% |
| 4 | Huawei | 24 | 4% |
| 5 | Vim | 14 | 2% |
| 6 | 青岛东胜伟业软件有限公司 | 14 | 2% |
| 7 | SourceCodester | 11 | 2% |
| 8 | Discourse | 10 | 2% |
| 9 | Lantronix | 10 | 2% |
| 10 | 其他 | 435 | 71% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 49 个电信行业漏洞，19 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“ASUS RT-AX86U 缓冲区溢出漏洞、Huawei S5700 和 S5800 拒绝服务漏洞、Omron CX-One 缓冲区溢出漏洞（CNVD-2022-04998）”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/

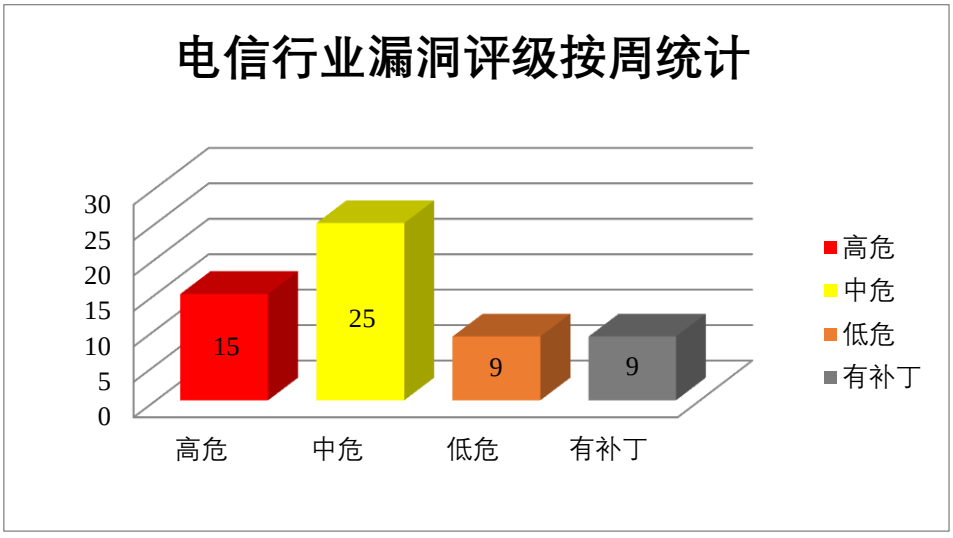


图 3 电信行业漏洞统计

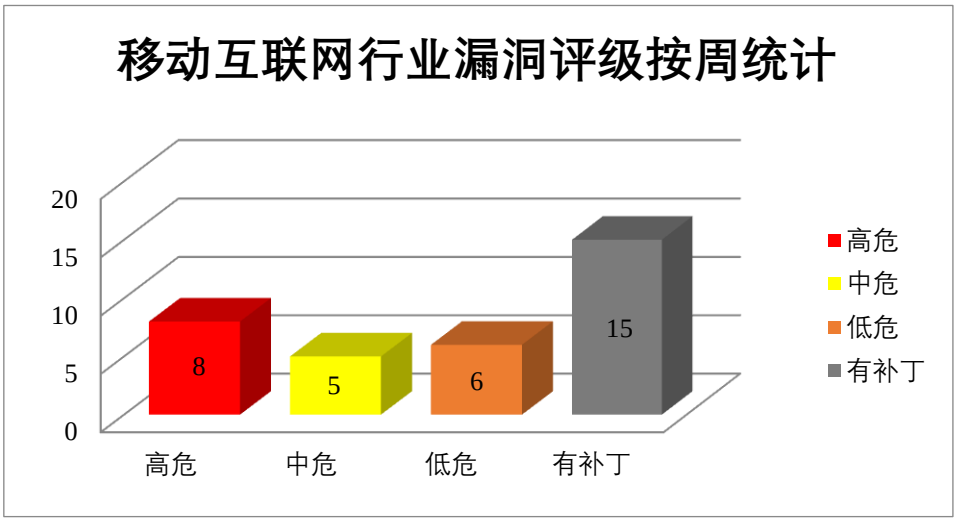


图 4 移动互联网行业漏洞统计

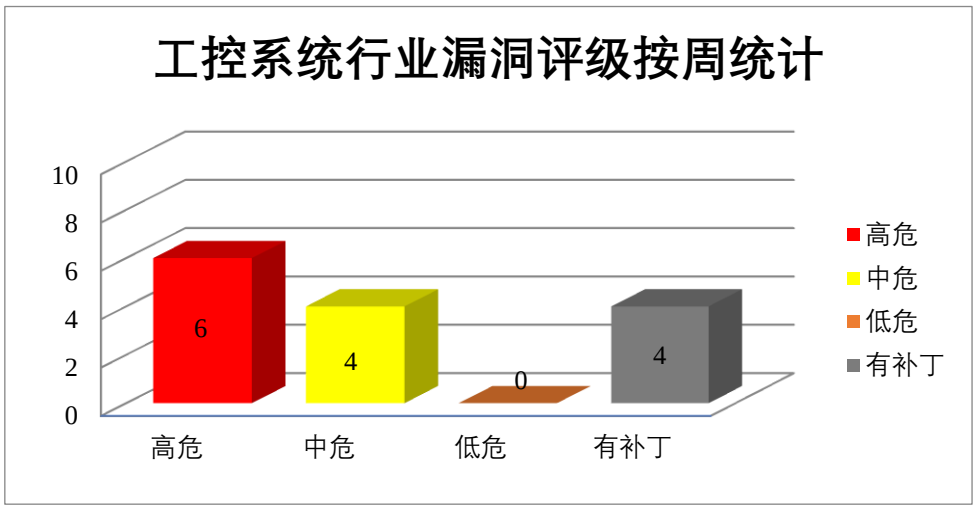


图 5 工控系统行业漏洞统计

## 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 Acrobat 是美国奥多比（Adobe）公司的一套 PDF 文件编辑和转换工具。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。Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。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任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat and Reader 资源管理错误漏洞（CNVD-2022-04528、CNVD-2022-04993、CNVD-2022-04991）、Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2022-04990）、Adobe Experience Manager 跨站脚本漏洞（CNVD

-2022-04999、CNVD-2022-05443）、Adobe Bridge 缓冲区溢出漏洞（CNVD-2022-05037）、Adobe Experience Manager 代码问题漏洞。其中，除“Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-04999）”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-2022-04528
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04990
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04993
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04991
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04999
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05037
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05443
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05442

### 2、Mozilla 产品安全漏洞

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从未初始化的内存位置读取数据，任意代码执行，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Rust messagepack-rs crate 文件读取漏洞（CNVD-2022-04511、CNVD-2022-04510）、Mozilla Rust 拒绝服务漏洞（CNVD-2022-04515）、Mozilla Rust 代码执行漏洞、Mozilla Rust ckb crate 拒绝服务漏洞、Mozilla Rust rdiff crate 文件读取漏洞、Mozilla Rust 内存破坏漏洞（CNVD-2022-04516）、Mozilla Rust 释放后重用漏洞。其中，除“Mozilla Rust rdiff crate 文件读取漏洞”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-2022-04511
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04510
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04515
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04514
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04513
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04512
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04516
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04519

### 3、Huawei 产品安全漏洞

Huawei S5700 和 Huawei S6700 都是中国华为（Huawei）公司的一款企业级交换机产品。Huawei Emui 是一款基于 Android 开发的移动端操作系统。Magic Ui 是一款基于

Android 开发的移动端操作系统。Huawei HarmonyOS Wearables 是中国华为（Huawei）公司的一款电子手表。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Huawei S5700 和 S5800 拒绝服务漏洞、Huawei EMUI 堆溢出漏洞、Huawei Emui 和 Magic UI 双重释放漏洞、Huawei Emui 和 Magic UI 配置缺陷漏洞、Huawei HarmonyOS Wearables 堆缓冲区溢出漏洞、Huawei HarmonyOS Wearables 越界写漏洞（CNVD-2022-05173、CNVD-2022-05172）、Huawei HarmonyOS Wearables 加密问题漏洞。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-2022-04713
https://www.cnvd.org.cn/flaw/show/CNVD-2022-04719
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05167
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05168
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05170
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05173
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05172
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05175

### 4、IBM 产品安全漏洞

IBM Security Secret Server 是一套特权访问管理解决方案。该产品支持密码管理、特权账号识别和特权会话访问监控记录等功能。IBM Security Guardium Data Encryption 是一个用于保护组织内敏感数据安全性的软件。IBM FileNet Content Manager 是一套针对 FileNet P8 平台的内容管理解决方案。该方案将文档管理与即用型工作流程工具相结合，可管理图像、视频、Web 内容、合规性文档等。IBM Spectrum Copy Data Management 是美国国际商业机器公司（IBM）的实现数据中心副本管理流程的现代化、简化和自动化。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，在受影响系统上执行任意 shell 命令。

CNVD 收录的相关漏洞包括：IBM Spectrum Copy Data Management 信息泄露漏洞（CNVD-2022-05081、CNVD-2022-05082）、IBM Spectrum Copy Data Management 输入验证错误漏洞、IBM Security Secret Server 信息泄露漏洞（CNVD-2022-05088、CNVD-2022-05090）、IBM Security Guardium Data Encryption 信息泄露漏洞（CNVD-2022-05124、CNVD-2022-05125）、IBM FileNet Content Manager 命令注入漏洞。其中，“IBM Spectrum Copy Data Management 输入验证错误漏洞”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-2022-05081
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05082
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05084
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05088
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05090
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05124
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05125
https://www.cnvd.org.cn/flaw/show/CNVD-2022-05430

### 5、ASUS DSL-N14U-B1 代码问题漏洞

ASUS DSL-N14U-B1 是中国华硕（ASUS）公司的一款路由器设备。本周，ASUS DSL-N14U-B1 被披露存在代码问题漏洞。攻击者可利用该漏洞上传任意文件内容作为固件更新。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-2022-04718

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.htm

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-2022-04714 | ASUS GT-AC2900 授权问题漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-Gaming-Routers/RT-AC2900/HelpDesk_BIOS/ |
| CNVD-2022-04981 | Lantronix PremierWave 2050 操作系统命令注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://talosintelligence.com/vulnerability_reports/TALOS-2021-1312 |
| CNVD-2022-05431 | Juniper Networks Junos OS 资源管理错误漏洞（CNVD-2022-05431） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://kb.juniper.net/InfoCenter/index?page=content&id=JSA11269&cat=SIRT_1&actp=LIST |
| CNVD-2022-05446 | Zoho ManageEngine Desktop Central MSP 授权问题漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：http://www.manageengine.com/desktop-management-msp/cve-2021-44515-security-advisory.html |

| | | | |
|---|---|---|---|
| CNVD-2022-05785 | Apache log4j Chainsaw 反序列化代码执行漏洞 | 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://logging.apache.org/chainsaw/2.x/download.html |
| CNVD-2022-05855 | PHPGurukul Apartment Visitors Management System SQL 注入漏洞 | 高 | 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://phpgurukul.com/apartment-visitors-management-system-using-php-and-mysql/ |
| CNVD-2022-05865 | Hitachi ABB Power Grids System Data Manager 加密问题漏洞 | 高 | 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://www.hitachiabb-powergrids.com/ch/en/offering/product-and-system/scada/microscada-x/sdm600 |
| CNVD-2022-05868 | Fortinet FortiManager 代码注入漏洞 | 高 | 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://www.fortinet.com/products/management/fortimanager |
| CNVD-2022-05874 | Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-05874） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.oracle.com/security-alerts/cpujan2022.html |
| CNVD-2022-05852 | Apache log4j JMSSink 反序列化代码执行漏洞 | 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://logging.apache.org/log4j/2.x/download.html |

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Mozilla、Huawei、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞从未初始化的内存位置读取数据，提升权限，任意代码执行，发起拒绝服务攻击等。另外，ASUS DSL-N14U-B1 被披露存在代码问题漏洞。攻击者可利用该漏洞上传任意文件内容作为固件更新。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、SeedDMS 跨站脚本漏洞（CNVD-2022-05448）

**验证描述**

SeedDMS 是一款免费文档管理系统，具有易于使用的基于 Web 的用户界面。

SeedDMS 6.0.7 版中的 AddEvent.php 组件存在跨站脚本漏洞。攻击者可通过名称和注释参数利用该漏洞注入恶意脚本代码。

**验证信息**

POC 链接：https://packetstormsecurity.com/files/165163/Auerswald-COMpact-8.0B-Privilege-Escalation.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-05448

**信息提供者**

华为技术有限公司

*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. Cisco StarOS 漏洞或有远程代码执行和信息泄露风险

日前，思科公司（Cisco）宣布修补了一项远程代码执行漏洞，该漏洞的追踪编号为 CVE-2022-20649，发现于公司旗下 StarOS 软件冗余配置管理器（RCM）中。

参考链接：https://www.freebuf.com/articles/320568.html

### 2. 研究人员在三种 WordPress 插件中发现高危漏洞

近日，WordPress 安全公司 Wordfence 的研究人员发现一项严重的漏洞，它可以作用于三种不同的 WordPress 插件，并已影响超过 84000 个网站。该漏洞的执行代码被追踪为 CVE-2022-0215，是一种跨站请求伪造（CSRF）攻击，通用安全漏洞评分系统（CVSS）对其给予 8.8 的评分。

参考链接：https://www.freebuf.com/articles/web/320123.html

**关于 CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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