国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 08 月 08 日-2022 年 08 月 14 日 **2022 年第 32 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 548 个，其中高危漏洞 158 个、中危漏洞 300 个、低危漏洞 90 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 275 个（占 50%），其中互联网上出现“PESCMS 跨站请求伪造漏洞（CNVD-2022-56093）、Online Fire Reporting System 跨站脚本漏洞”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 5952 个，与上周（6731 个）环比减少 12%。

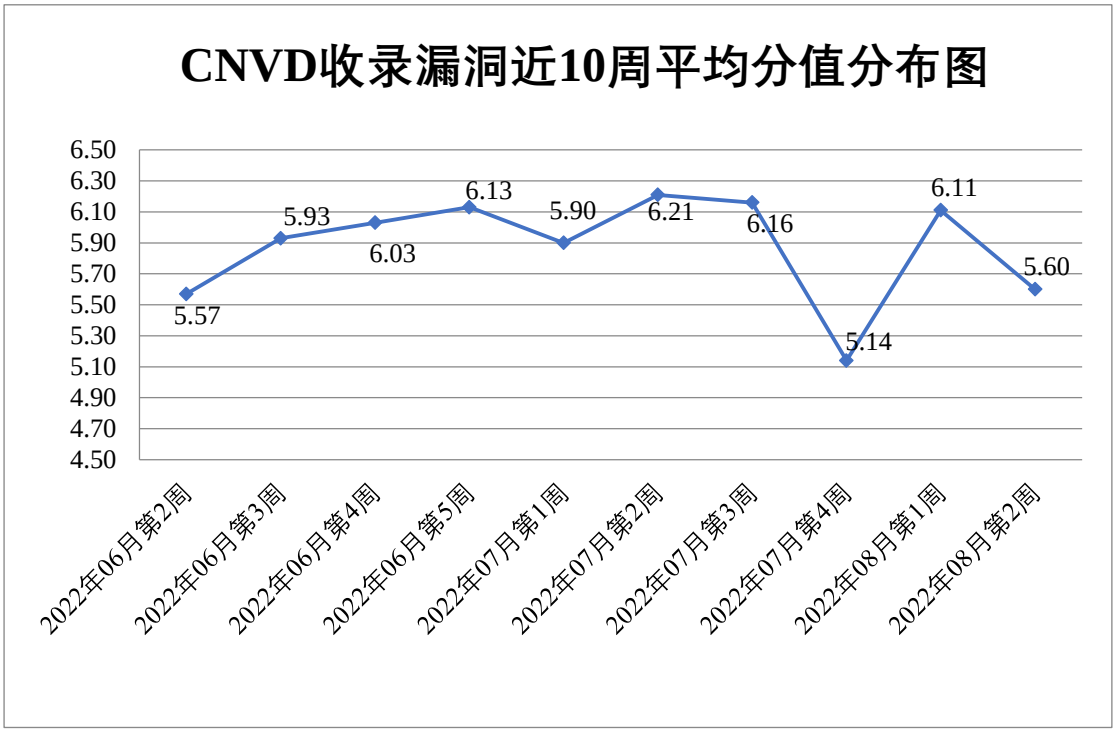

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 19 起，向基础电信企业通报漏洞事件 15 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 504 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 127 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 50 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：

珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆涅若科技有限公司、重庆路西法科技有限公司、众勤通信设备贸易（上海）有限公司、中微达科技有限公司、中山市同创科技发展有限公司、中科方德软件有限公司、浙江正裕工业股份有限公司、浙江臻善科技股份有限公司、浙江大华技术股份有限公司、长沙博为软件技术股份有限公司、云顶信息技术股份有限公司、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、夏普商贸（中国）有限公司、暇光软件科技（上海）有限公司、西安众邦网络科技有限公司、西安新软信息科技有限公司、武汉新宏博科技有限公司、微软（中国）有限公司、网经科技（苏州）有限公司、天津天堰科技股份有限公司、苏州天一信德环保科技有限公司、苏州市亿韵商务信息有限公司、苏州科达科技股份有限公司、苏州浩辰软件股份有限公司、苏州国网电子科技有限公司、四平市九州易通科技有限公司、施耐德电气(中国)有限公司、神州数码信息服务股份有限公司、深圳智慧光迅信息技术有限公司、深圳市迅捷通信技术有限公司、深圳市万网博通科技有限公司、深圳市明源云科技有限公司、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、上海卓卓网络科技有限公司、上海晓材科技有限公司、上海三高计算机中心股份有限公司、上海青枣网络科技有限公司、上海穆云智能科技有限公司、上海亘岩网络科技有限公司、上海泛微网络科技股份有限公司、上海二三四五网络科技有限公司、熵基科技股份有限公司、山东中维世纪科技股份有限公司、山东潍微科技股份有限公司、山东山大华天软件有限公司、山东欧倍尔软件科技有限责任公司、厦门网中网软件有限公司、南京云网汇联软件技术有限公司、南昌蓝智科技有限公司、茉柏枘（上海）软件科技有限公司、摩莎科技（上海）有限公司、明腾网络股份有限公司、迈普通信技术股份有限公司、零视技术(上海)有限公司、猎豹移动公司、理光（中国）投资有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、京迈（湖北）电子商务有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、江苏知途教育科技有限公司、江苏省广电有线信息网络股份有限公司、江苏三希科技股份有限公司、佳能（中国）有限公司、济南中维世纪科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖北淘码千维信息科技有限公司、恒锋信息科技股份有限公司、合肥盛东信息科技有限公司、杭州易软共创网络科技有限公司、杭州叙简科技股份有限公司、杭州思福迪信息技术有限公

司、杭州三汇信息工程有限公司、海南驰豹科技有限公司、国交信息股份有限公司、桂林崇胜网络科技有限公司、贵州筑站信息技术有限公司、广州中望龙腾软件股份有限公司、广州图创计算机软件开发有限公司、广州南方卫星导航仪器有限公司、广州浩洋信息科技有限公司、广西计算中心有限责任公司、广联达科技股份有限公司、广东飞企互联科技股份有限公司、烽火通信科技股份有限公司、帆软软件有限公司、东莞市东城乔伦软件开发工作室、东莞市东城飞飞网络科技经营部、稻田共享信息技术石家庄有限公司、郸城县新翔软件科技有限公司、戴尔（中国）有限公司、大唐电信科技股份有限公司、大连华天软件有限公司、成都云腾五洲科技有限公司、成都佳发安泰教育科技股份有限公司、成都飞鱼星科技股份有限公司、北京中科网威信息技术有限公司、北京智慧远景科技产业有限公司、北京致远互联软件股份有限公司、北京用友融联科技有限公司、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、北京网御星云信息技术有限公司、北京网梯科技发展有限公司、北京网康科技有限公司、北京通达志成科技有限公司、北京数字政通科技股份有限公司、北京全品文教科技股份有限公司、北京龙软科技股份有限公司、北京领雾科技有限公司、北京酷我科技有限公司、北京九思协同软件有限公司、北京竞业达数码科技股份有限公司、北京火星高科数字科技有限公司、北京飞书科技有限公司、北京棣南新宇科技有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、暴风集团股份有限公司、安徽晶奇网络科技股份有限公司、爱普生（中国）有限公司、信呼、华夏 ERP、zzzcms、ZZCMS、XnSoft、Witte Software、ThinkItCMS、SEMCMS、FTCMS、Fernhill Software、Belkin International,Inc 和 Axis Communications AB.。

本周，CNVD 发布了《Microsoft 发布 2022 年 8 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7986

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、天津市国瑞数码安全系统股份有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、中国电信股份有限公司网络安全产品运营中心、河南信安世纪科技有限公司、贵州泰若数字科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、山石网科通信技术股份有限公司、杭州迪普科技股份有限公司、星云博创科技有限公司、西门子（中国）有限公司、浙江木链物联网科技有限公司、平安银河实验室、广州安亿信软件科技有限公司、江苏天竞云合数据技术有限公司、上海纽盾科技股份有限公司、北京威努特技术有限公司、苏州棱镜七彩信息科技有限公司、重庆都会信

息科技、北京六方云信息技术有限公司、福建省海峡信息技术有限公司、内蒙古洞明科技有限公司、河南灵创电子科技有限公司、博智安全科技股份有限公司、江苏耘和计算机系统工程有限公司、山东新潮信息技术有限公司、北京百度网讯科技有限公司、中科汇能科技有限公司、广电奇安网络科技（重庆）有限公司、黑龙江亿林网络股份有限公司、上海嘉韦思信息技术有限公司、京数安（北京）科技有限公司及其他个人白帽子向 CNVD 提交了 5952 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、奇安信网神（补天平台）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 4573 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
奇安信网神（补天平台）	2077	2077
三六零数字安全科技集团有限公司	1168	1168
斗象科技（漏洞盒子）	1070	1070
北京神州绿盟科技有限公司	389	2
新华三技术有限公司	369	0
上海交大	258	258
深信服科技股份有限公司	257	2
安天科技集团股份有限公司	227	0
天津市国瑞数码安全系统股份有限公司	171	0
北京天融信网络安全技术有限公司	110	3
恒安嘉新（北京）科技股份公司	104	0
北京启明星辰信息安全技术有限公司	89	32
杭州安恒信息技术股份有限公司	89	89
北京数字观星科技有限公司	80	0
南京众智维信息科技有限公司	29	29
西安四叶草信息技术有限公司	12	12
北京知道创宇信息技术有限公司	9	0

深圳市腾讯计算机系统有限公司（玄武实验室）	4	4
内蒙古奥创科技有限公司	3	3
南京联成科技发展股份有限公司	3	3
北京智游网安科技有限公司	2	2
北京华顺信安科技有限公司	224	4
中国电信股份有限公司网络安全产品运营中心	38	38
河南信安世纪科技有限公司	37	37
贵州泰若数字科技有限公司	24	24
奇安星城网络安全运营服务（长沙）有限公司	19	19
河南东方云盾信息技术有限公司	18	18
山石网科通信技术股份有限公司	15	15
杭州迪普科技股份有限公司	14	0
星云博创科技有限公司	9	9
西门子（中国）有限公司	7	0
浙江木链物联网科技有限公司	6	6
平安银河实验室	6	6
广州安亿信软件科技有限公司	4	4
江苏天竞云合数据技术有限公司	3	3
上海纽盾科技股份有限公司	3	3
北京威努特技术有限公司	2	2
苏州棱镜七彩信息科	2	2

技有限公司		
重庆都会信息科技	2	2
北京六方云信息技术有限公司	2	2
福建省海峡信息技术有限公司	2	2
内蒙古洞明科技有限公司	2	2
河南灵创电子科技有限公司	1	1
博智安全科技股份有限公司	1	1
江苏耘和计算机系统工程有限公司	1	1
山东新潮信息技术有限公司	1	1
北京百度网讯科技有限公司	1	1
中科汇能科技有限公司	1	1
中国工商银行	1	1
广电奇安网络科技（重庆）有限公司	1	1
黑龙江亿林网络股份有限公司	1	1
中国银行	1	1
上海嘉韦思信息技术有限公司	1	1
京数安（北京）科技有限公司	1	1
北京奇虎测腾科技有限公司	1	0
CNCERT 内蒙古分中心	2	2
CNCERT 宁夏分中心	1	1
个人	985	985
报送总计	7960	5952

本周漏洞按类型和厂商统计

本周，CNVD 收录了 548 个漏洞。WEB 应用 257 个，应用程序 174 个，网络设备（交换机、路由器等网络端设备）73 个，智能设备（物联网终端设备）33 个，安全产品 6 个，操作系统 5 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	257
应用程序	174
网络设备（交换机、路由器等网络端设备）	73
智能设备（物联网终端设备）	33
安全产品	6
操作系统	5

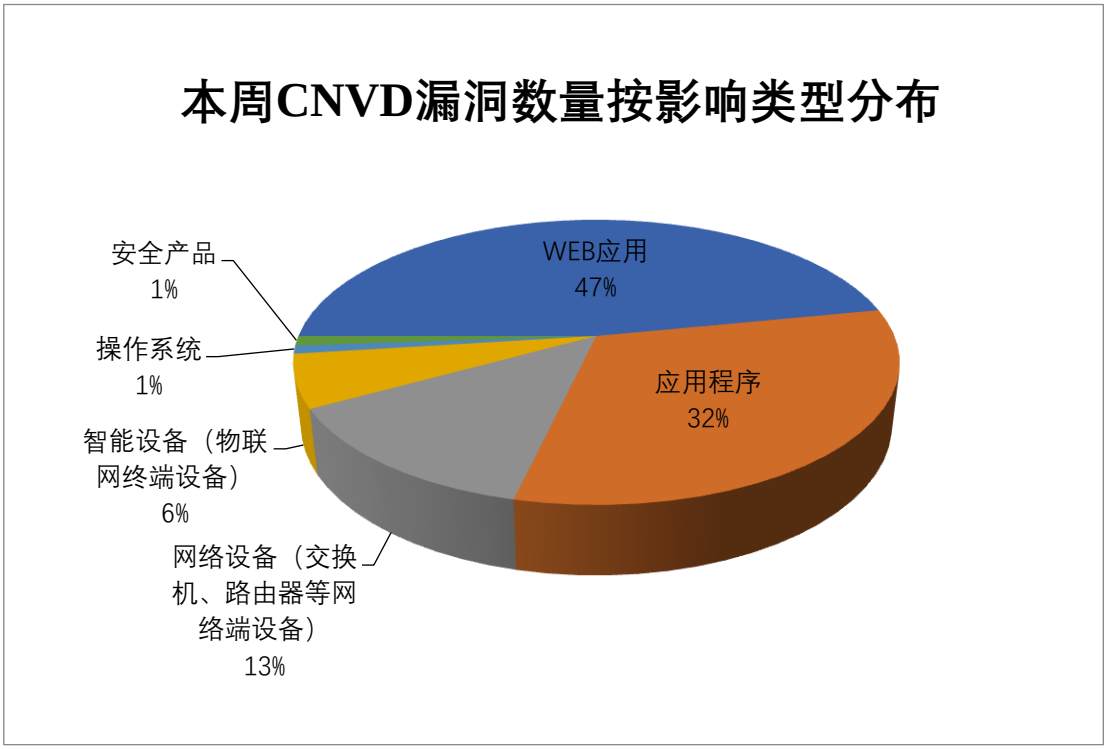

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Microsoft、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	WordPress	100	18%
2	Microsoft	28	5%
3	Adobe	21	4%
4	Tenda	19	3%
5	D-Link	19	3%
6	IBM	19	3%
7	Online Ordering System	15	3%
8	Carlo Montero	14	3%
9	TOTOLINK	13	3%

10	其他	300	55%

本周行业漏洞收录情况

本周，CNVD 收录了 60 个电信行业漏洞，15 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Cisco Small Business 缓冲区溢出漏洞（CNVD-2022-56085）、D-Link DSL-3782 缓冲区溢出漏洞（CNVD-2022-56666）”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/

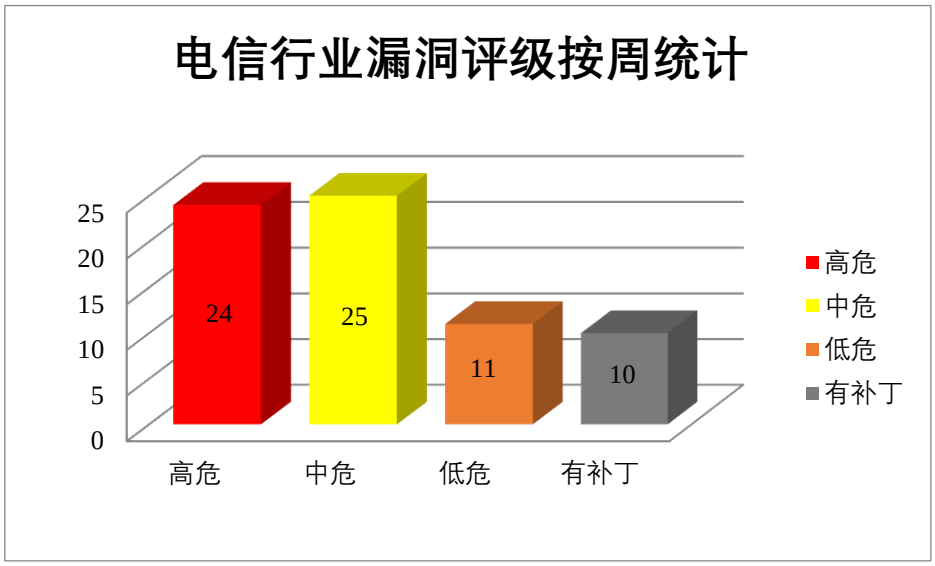

图 3 电信行业漏洞统计

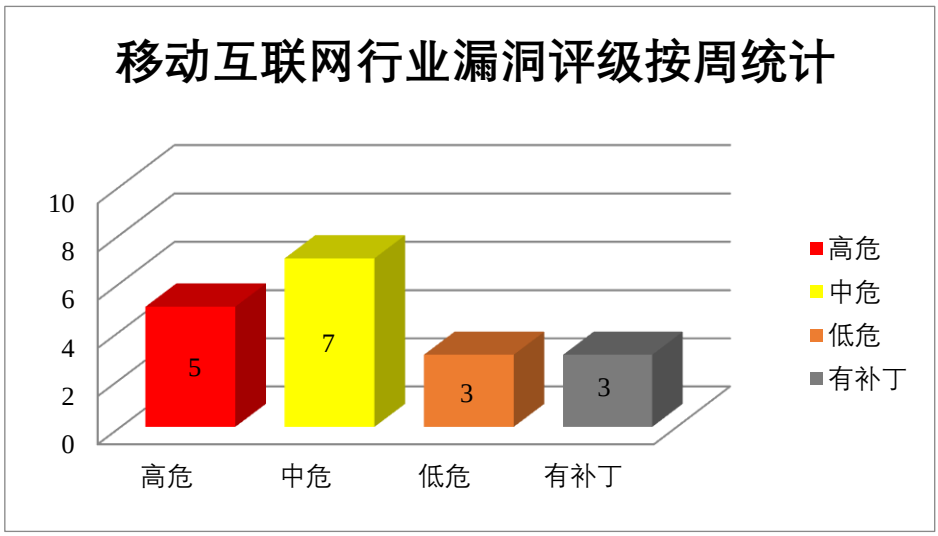

图 4 移动互联网行业漏洞统计

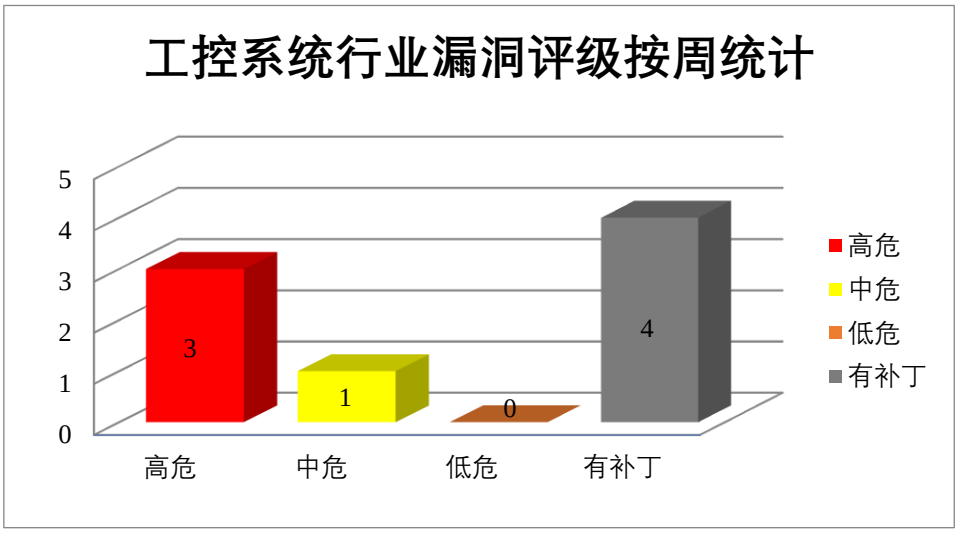

图 5 工控系统行业漏洞统计

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 PowerVM VIOS 是美国万国商业机器（IBM）的一个位于逻辑分区中的软件。该软件有助于在服务器内的客户端逻辑分区之间共享物理 I/O 资源。IBM Security Verify Information Queue 是美国 IBM 公司的一个集成产品。利用 Kafka 技术和发布/订阅模型来集成 IBM Security 产品之间的数据。IBM Robotic Process Automation 是美国 IBM 公司的一种机器人流程自动化产品。可帮助您以传统 RPA 的轻松和速度大规模自动化更多业务和 IT 流程。IBM QRadar Network Security 是美国 IBM 公司的一个网络安全管理器。用于提供对网络上的活动和用户的更好的可见性和控制，同时使用深度数据包检查、启发式和基于行为的分析来检测和预防高级威胁。IBM Spectrum Protect Operations Center 是美国 IBM 公司的一个为 IBM Spectrum Protect 环境提供可视化控制的软件。IBM CICS TX Advanced 是美国 IBM 公司的一个综合的、单一的事务运行时包。可以为独立应用程序提供云原生部署模型。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪造恶意请求诱骗受害者点击执行敏感操作，可以获得登录访问令牌，篡改系统配置或导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM PowerVM VIOS 拒绝服务漏洞、IBM Security Verify Information Queue 跨站请求伪造漏洞（CNVD-2022-55633）、IBM Robotic Process Automation 访问控制错误漏洞、IBM QRadar Network Security 信任管理问题漏洞、IBM QRadar Network Security 信息泄露漏洞（CNVD-2022-55637）、IBM Spectrum Protect Operations Center 暴力破解漏洞、IBM Robotic Process Automation 信息泄露漏洞（CNVD-2022-55663）、IBM CICS TX Advanced 访问控制错误漏洞。其中，“IBM

PowerVM VIOS 拒绝服务漏洞、IBM Spectrum Protect Operations Center 暴力破解漏洞”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-2022-55629

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55633

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55632

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55636

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55637

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55664

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55663

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56086

2、 Adobe 产品安全漏洞

Adobe InCopy 是美国 Adobe 公司的一款用于创作的文本编辑软件。Adobe Acrobat 和 Adobe Reader 都是美国奥多比（Adobe）公司的产品。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过特制数据可以触发超过分配缓冲区末尾的写入，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Adobe InCopy 缓冲区溢出漏洞（CNVD-2022-55642、CNVD-2022-55644）、Adobe Acrobat 和 Adobe Reader 资源管理错误漏洞（CNVD-2022-56090、CNVD-2022-56092、CNVD-2022-56258）、Adobe Acrobat 和 Adobe Reader 缓冲区溢出漏洞（CNVD-2022-56132、CNVD-2022-56130、CNVD-2022-56133）。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-2022-55642

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55644

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56090

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56092

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56132

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56130

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56133

https://www.cnvd.org.cn/flaw/show/CNVD-2022-56258

3、 Siemens 产品安全漏洞

Simcenter STAR-CCM+是一个多物理计算流体动力学（CFD）软件，用于模拟在真实世界条件下运行的产品。SCALANCE M-800、MUM-800 和 S615 以及 RUGGEDCOM RM1224 工业路由器用于通过移动网络（如 GPRS 或 UMTS）安全远程访问工厂，并

具有防火墙的集成安全功能，以防止未经授权的访问，以及 VPN 来保护数据传输。SCALANCE SC-600 设备（SC622-2C、SC632-2C、SC636-2C，SC642-2C、SC646-2C）用于保护受信任的工业网络免受不受信任的网络攻击。它们允许以不同的方式过滤传入和传出网络连接。SCALANCE W-1700 产品是基于 IEEE 802.11ac 标准的无线通信设备。SCALANCE W-700 产品是基于 IEEE 802.11ax 标准的无线通信设备。SCALANCE X switches 用于连接工业部件，如可编程逻辑控制器（PLC）或人机接口（HMI）。Siemens Comos 是德国西门子（Siemens）公司的一个工厂工程软件解决方案。用于过程工业。Siemens Syngo FastView 是德国西门子（Siemens）公司的一个 Dicom 交换媒体上提供的 Dicom 2 图像的独立查看器。Teamcenter 软件是一个现代化的、适应性强的产品生命周期管理 (PLM) 系统，它通过数字线程将人员和流程跨功能孤岛连接起来，以实现创新。SICAM A8000 RTU（远程终端装置）系列是一个模块化设备系列，适用于所有能源供应领域的远程控制和自动化应用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从组件（如内部网络拓扑或连接的系统）检索调试级别信息，执行远程代码，造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Siemens Teamcenter 命令注入漏洞、Siemens Teamcenter 拒绝服务漏洞、Siemens SICAM A8000 Web Server Module 身份验证绕过漏洞、Siemens Simcenter STAR-CCM+信息泄露漏洞、Siemens SCALANCE 产品命令注入漏洞、Siemens Comos 代码问题漏洞、Siemens Syngo FastView 越界写入漏洞（CNVD-2022-56511、CNVD-2022-56512）。其中，“Siemens Teamcenter 命令注入漏洞、Siemens Teamcenter 拒绝服务漏洞、Siemens SCALANCE 产品命令注入漏洞、Siemens Syngo FastView 越界写入漏洞（CNVD-2022-56511、CNVD-2022-56512）”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-2022-56473
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56472
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56478
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56477
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56476
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56510
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56511
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56512

4、 JetBrains 产品安全漏洞

JetBrains TeamCity 是捷克 JetBrains 公司的一套分布式构建管理和持续集成工具。该工具提供持续单元测试、代码质量分析和构建问题分析报告等功能。JetBrains IntelliJ IDEA 是捷克 Jetbrains 公司的一套适用于 Java 语言的集成开发环境。JetBrains Rider

是捷克 Jetbrains 公司的一套跨平台的.NET 集成开发环境（IDE）。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，通过自定义 JSON 模式中的 HTML 描述执行本地代码等。

CNVD 收录的相关漏洞包括：JetBrains TeamCity 日志信息泄露漏洞、JetBrains TeamCity 跨站脚本漏洞（CNVD-2022-55670）、JetBrains IntelliJ IDEA 代码注入漏洞（CNVD-2022-55675、CNVD-2022-55674、CNVD-2022-55680、CNVD-2022-55681）、JetBrains IntelliJ IDEA 跨站脚本漏洞、JetBrains Rider 代码注入漏洞。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-2022-55671
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55670
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55675
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55674
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55680
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55679
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55677
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55681

5、Tenda M3 formMasterMng 函数堆栈溢出漏洞

Tenda M3 是中国腾达（Tenda）公司的一款门禁控制器。本周，Tenda M3 被披露存在函数堆栈溢出漏洞。攻击者可利用该漏洞导致拒绝服务攻击。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-2022-56548

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-2022-55630	Apache Calcite 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/5csdj8bv4h3hfgw27okm84jh1j2fyw0c
CNVD-2022-55640	Apache CloudStack XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/hwhxvtwp1d5dsm156bsf1cnyvtmrfv3f
CNVD-2022-55641	Apache SkyWalking 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://lists.apache.org/thread/x238w

			o4r5goy39dxdjcmlofp6gcdnqr3
CNVD-2022-55645	Adobe InDesign 缓冲区溢出漏洞（CNVD-2022-55645）	高	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/apsb22-30.html
CNVD-2022-55648	Apache Hive 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://lists.apache.org/thread/oqqgnhz4c6nxsfd0xstosnk0g15f7354
CNVD-2022-55647	Adobe InDesign 缓冲区溢出漏洞（CNVD-2022-55647）	高	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/apsb22-30.html
CNVD-2022-55682	多款 Cisco Small Business 产品拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-overflow-s2r82P9v
CNVD-2022-55694	WordPress 插件 KiviCare SQL 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://wpscan.com/vulnerability/53f493e9-273b-4349-8a59-f2207e8f8f30
CNVD-2022-55700	WordPress Member Hero plugin 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpscan.com/vulnerability/8b08b72e-5584-4f25-ab73-5ab0f47412df
CNVD-2022-55714	Online Ordering System SQL 注入漏洞（CNVD-2022-55714）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcecodester.com/php/5125/online-ordering-system-using-phpmysql.html

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞伪造恶意请求诱骗受害者点击执行敏感操作，可以获得登录访问令牌，篡改系统配置或导致拒绝服务等。此外，Adobe、Siemens、JetBrains 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过特制数据可以触发超过分配缓冲区末尾的写入，在系统上执行任意代码，导致拒绝服务等。另外，Tenda M3 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞导致拒绝服务攻击。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、PESCMS 跨站请求伪造漏洞（CNVD-2022-56093）

验证描述

PESCMS 是一个内容发布平台。

PESCMS V2.3.3 版本存在安全漏洞。攻击者利用该漏洞删除用户公司的相关信息。

验证信息

POC 链接：https://github.com/RO6OTXX/pescms_vulnerability

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-56093

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. Instagram 被曝通过 App 内浏览器跟踪用户网络活动

IT 之家 8 月 14 日消息，对 Meta 旗下 Instagram 应用程序的一项新分析表明，每次用户点击应用程序内的链接时，Instagram 都能够监控他们的所有交互、文本选择，甚至是文本输入，例如内部网站内密码和私人信用卡详细信息应用程序。

参考链接：https://www.ithome.com/0/634/976.htm

2. 利用 macOS 端 Zoom 安装器漏洞，黑客可接管用户 Mac

一名安全专家近日发现利用 macOS 端 Zoom 应用程序，掌控整个系统权限的攻击方式。上周五在拉斯维加斯召开的 Def Con 黑客大会上，Mac 安全专家帕特里克·沃德尔（Patrick Wardle）在演讲中详细介绍了这个漏洞细节。

参考链接：https://www.cnbeta.com/articles/tech/1304009.htm

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