国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 09 月 12 日-2022 年 09 月 18 日 **2022 年第 37 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 347 个，其中高危漏洞 146 个、中危漏洞 151 个、低危漏洞 50 个。漏洞平均分值为 6.02。本周收录的漏洞中，涉及 0day 漏洞 236 个（占 68%），其中互联网上出现“SourceCodester Bank Management System SQL 注入漏洞、Social Codia SMS 任意文件上传漏洞”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 12967 个，与上周（7225 个）环比增加 79%。

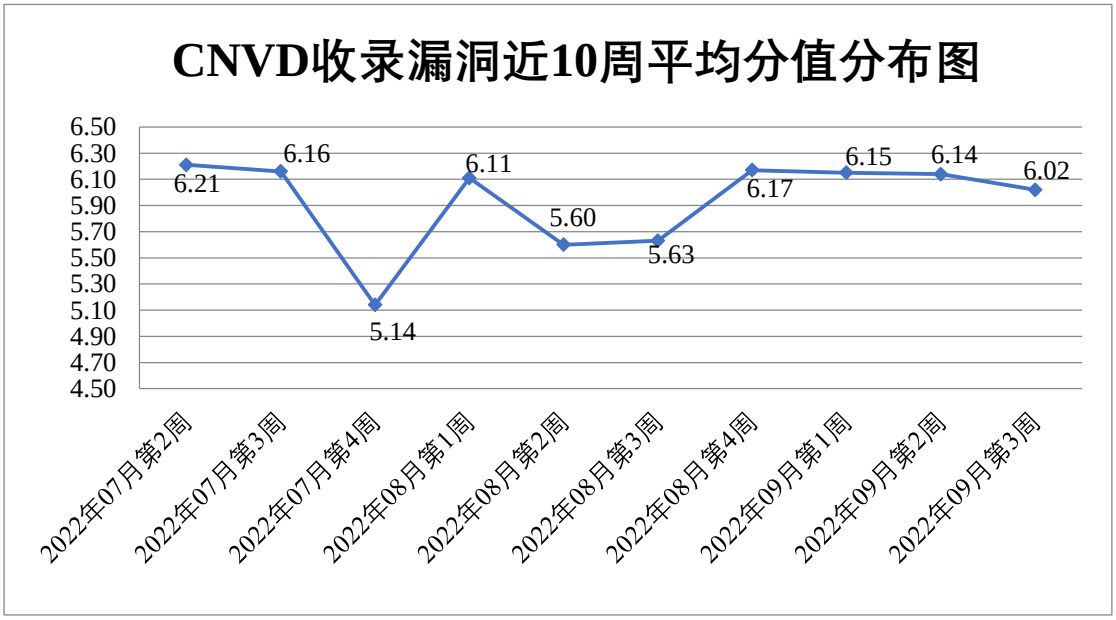

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 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 797 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 182 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 91 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：

重庆森鑫炬科技有限公司、郑州冰川网络技术有限公司、正方软件股份有限公司、友讯电子设备（上海）有限公司、优慕课在线教育科技（北京）有限责任公司、用友网络科技股份有限公司、新疆恒和久远信息技术有限公司、心品网络科技有限公司、西安凤巢网络科技有限公司、温州市万旗信息科技有限公司、微试云（安徽）医疗信息有限公司、苏州浩辰软件股份有限公司、沈阳明致软件有限公司、沈阳宏景世纪软件有限公司、神州数码集团股份有限公司、深圳市利谱信息技术有限公司、深圳市蓝凌软件股份有限公司、深圳市科图自动化新技术有限公司、深圳市吉祥腾达科技有限公司、深圳市华域数安科技有限公司、深圳市步科电气有限公司、深圳市必联电子有限公司、深圳警翼智能科技股份有限公司、上海展盟网络科技有限公司、上海新萌网络科技有限公司、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、山东中维世纪科技股份有限公司、山东中创软件商用中间件股份有限公司、山东欧倍尔软件科技有限责任公司、厦门市佳庆网络科技有限公司、润申信息科技（上海）有限公司、联奕科技股份有限公司、乐星电气（无锡）有限公司、朗坤智慧科技股份有限公司、卡莱特云科技股份有限公司、济南时空超越科技有限公司、吉翁电子（深圳）有限公司、华硕电脑（上海）有限公司、湖南壹拾捌号网络技术有限公司、恒锋信息科技股份有限公司、杭州映云科技有限公司、杭州图南电子股份有限公司、杭州三汇信息工程有限公司、杭州海康威视数字技术股份有限公司、海南赞赞网络科技有限公司、哈尔滨新中新电子股份有限公司、广州市扬海数码科技有限公司、广州市领课网络科技有限公司、广州市高科通信技术股份有限公司、广州凝智科技有限公司、福州联讯信息科技有限公司、福建星网锐捷通讯股份有限公司、福建福昕软件开发股份有限公司、大唐电信科技股份有限公司、大连华天软件有限公司、大连大有吴涛易语言软件开发有限公司、成都赛新科技有限公司、成都任我行软件股份有限公司、畅捷通信息技术股份有限公司、比亚迪股份有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京通达信科科技有限公司、北京数字政通科技股份有限公司、北京数科网维技术有限责任公司、北京派网软件有限公司、北京九思协同软件有限公司、北京点聚信息技术有限公司、北京步鼎方舟科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、安美世纪（北京）科技有限公司、安徽协达软件科技有限公司、安徽青柿信息科技有限公司、若依、TOTOLINK 和 KYOCERA。

本周，CNVD 发布了《Microsoft 发布 2022 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8106

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、阿里云计算有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、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。北京华顺信安信息技术有限公司、杭州默安科技有限公司、杭州迪普科技股份有限公司、北京山石网科信息技术有限公司、河南东方云盾信息技术有限公司、山东云天安全技术有限公司、山石网科通信技术股份有限公司、河南信安世纪科技有限公司、中国电信股份有限公司网络安全产品运营中心、北京安帝科技有限公司、重庆都会信息科技有限公司、苏州棱镜七彩信息科技有限公司、山东新潮信息技术有限公司、任子行网络技术股份有限公司、快页信息技术有限公司、广东唯顶信息科技股份有限公司、北京升鑫网络科技有限公司、广东默究科技有限公司、河北千诚电子科技有限公司、上海上讯信息技术股份有限公司、广州安亿信软件科技有限公司、星云博创科技有限公司、北京君云天下科技有限公司、云南联创网安科技有限公司、上海纽盾科技股份有限公司、浙江木链物联网科技有限公司、河南悦海数安科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、湖南省金盾信息安全等级保护评估中心有限公司、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 12967 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）、三六零数字安全科技集团有限公司、奇安信网神（补天平台）和上海交大向 CNVD 共享的白帽子报送的 11275 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）	6007	6007
斗象科技（漏洞盒子）	3661	3661
三六零数字安全科技集团有限公司	1232	1232
深信服科技股份有限公司	420	0
阿里云计算有限公司	395	0
上海交大	375	375
新华三技术有限公司	329	0
北京天融信网络安全技术有限公司	259	5

北京神州绿盟科技有限公司	216	8
安天科技集团股份有限公司	202	0
南京众智维信息科技有限公司	154	154
恒安嘉新（北京）科技股份公司	107	0
杭州安恒信息技术股份有限公司	87	79
北京数字观星科技有限公司	75	0
北京启明星辰信息安全技术有限公司	60	2
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	44	44
中国电信集团系统集成有限责任公司	30	0
西门子（中国）有限公司	24	0
京东科技信息技术有限公司	20	0
北京知道创宇信息技术有限公司	15	2
北京长亭科技有限公司	6	6
沈阳东软系统集成工程有限公司	5	5
远江盛邦（北京）网络安全科技股份有限公司	5	5
南京联成科技发展股份有限公司	3	3

北京华顺信安信息技术有限公司	216	6
杭州默安科技有限公司	37	37
杭州迪普科技股份有限公司	28	2
北京山石网科信息技术有限公司	20	20
河南东方云盾信息技术有限公司	19	19
山东云天安全技术有限公司	15	15
山石网科通信技术股份有限公司	10	10
河南信安世纪科技有限公司	7	7
中国电信股份有限公司网络安全产品运营中心	6	6
北京安帝科技有限公司	4	4
重庆都会信息科技有限公司	4	4
苏州棱镜七彩信息科技有限公司	4	4
山东新潮信息技术有限公司	4	4
任子行网络技术股份有限公司	4	4
快页信息技术有限公司	3	3
广东唯顶信息科技股份有限公司	3	3
北京升鑫网络科技有限公司	3	3

广东默究科技有限公司	3	3
河北千诚电子科技有限公司	2	2
上海上讯信息技术股份有限公司	2	2
广州安亿信软件科技有限公司	2	2
星云博创科技有限公司	2	2
北京君云天下科技有限公司	1	1
云南联创网安科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
浙江木链物联网科技有限公司	1	1
河南悦海数安科技有限公司	1	1
奇安星城网络安全运营服务（长沙）有限公司	1	1
湖南省金盾信息安全等级保护评估中心有限公司	1	1
北京机沃科技有限公司	1	1
CNCERT 浙江分中心	1	1
CNCERT 贵州分中心	1	1
个人	1207	1207
报送总计	15405	12967

本周漏洞按类型和厂商统计

本周，CNVD 收录了 347 个漏洞。WEB 应用 177 个，应用程序 113 个，网络设备（交换机、路由器等网络端设备）25 个，操作系统 12 个，智能设备（物联网终端设备）9 个，安全产品 9 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
WEB 应用	177
应用程序	113
网络设备（交换机、路由器等网络端设备）	25
操作系统	12
智能设备（物联网终端设备）	9
安全产品	9
数据库	2

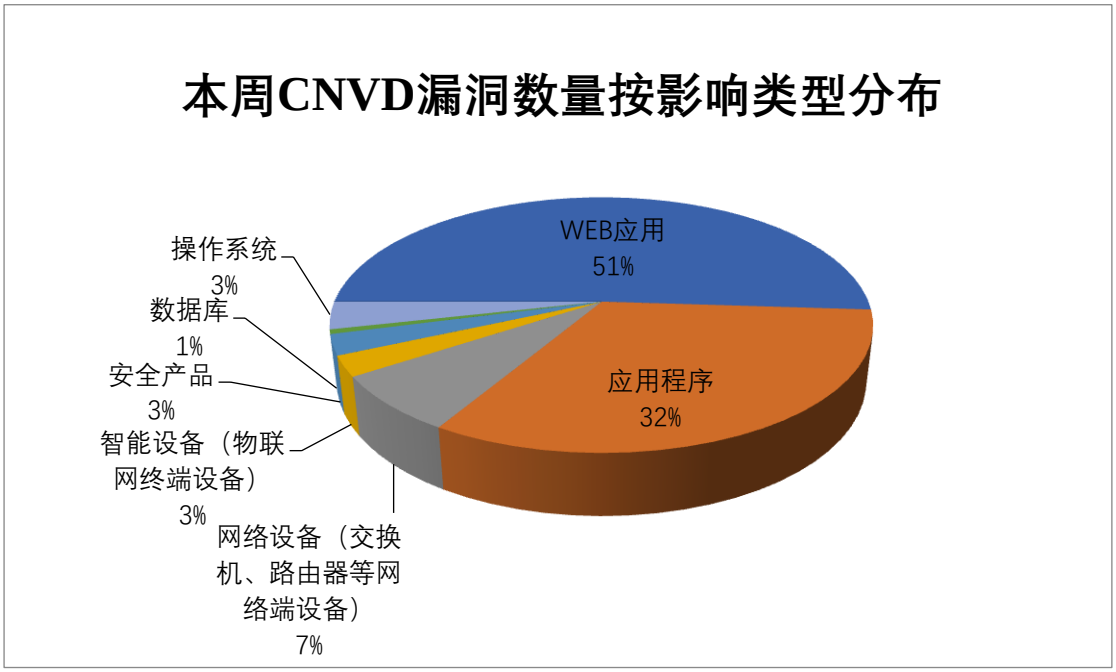

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Samsung、Siemens、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	Samsung	30	9%
2	Siemens	23	6%
3	IBM	13	4%
4	SAP	11	3%
5	WordPress	10	3%

6	Microsoft	7	2%
7	深圳市吉祥腾达科技有限公司	7	2%
8	TOTOLINK	6	2%
9	迈普通信技术股份有限公司	6	2%
10	其他	234	67%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，19 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Elcomplus SmartPPT 授权问题漏洞、Elcomplus SmartPPT 信息泄露漏洞”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/

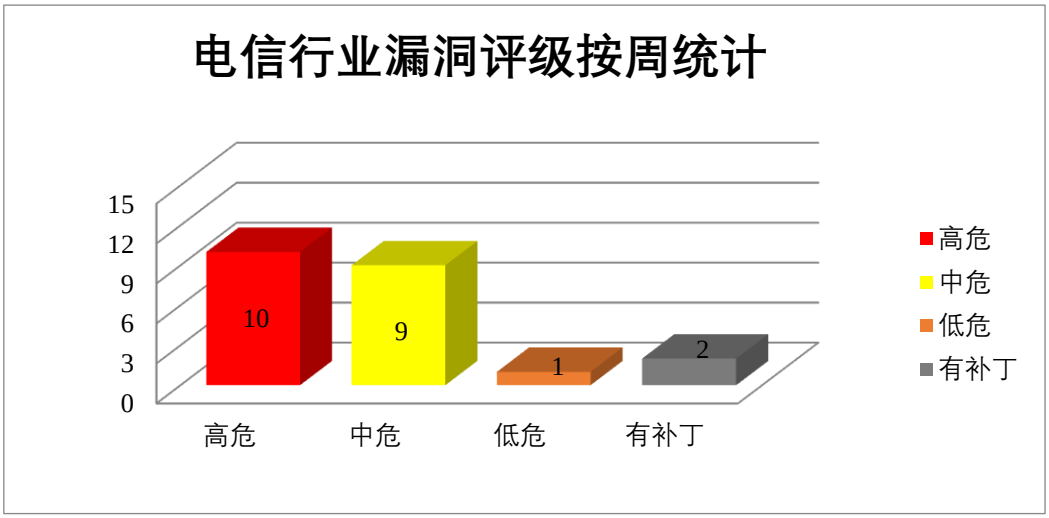

图 3 电信行业漏洞统计

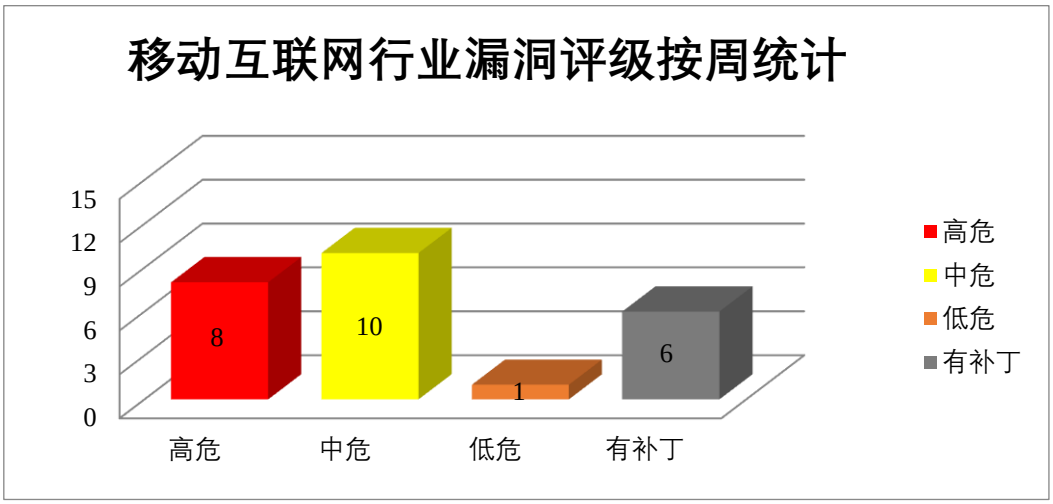

图 4 移动互联网行业漏洞统计

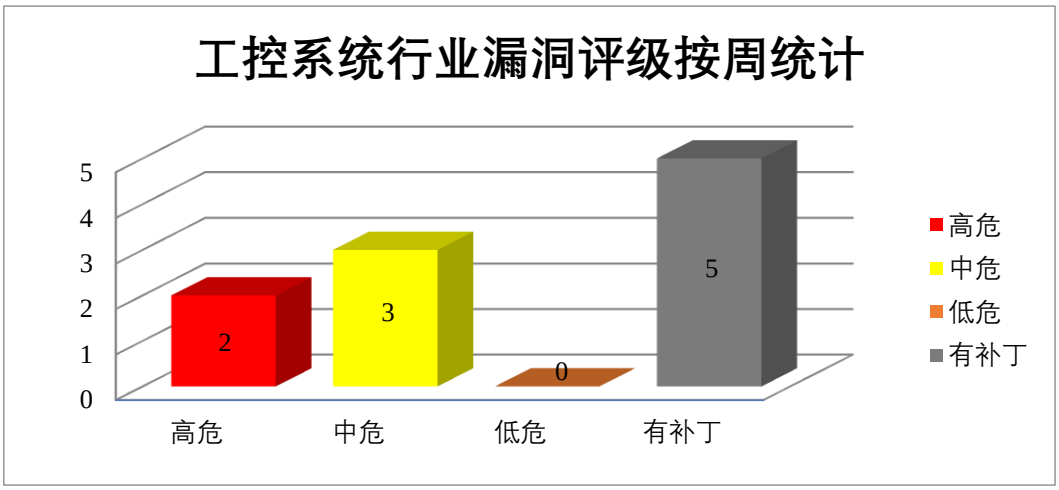

图 5 工控系统行业漏洞统计

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、 Samsung 产品安全漏洞

Samsung SMR 是韩国三星（Samsung）公司的一个系统补丁包。提供了三星手机应用的补丁程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞启动某些活动，进行越界写入，执行代码等。

CNVD 收录的相关漏洞包括：Samsung SMR 输入验证错误漏洞（CNVD-2022-63630、CNVD-2022-63647）、Samsung SMR 缓冲区溢出漏洞（CNVD-2022-63652）、Samsung SMR 堆缓冲区溢出漏洞（CNVD-2022-63631、CNVD-2022-63655、CNVD-2022-63658、CNVD-2022-63656、CNVD-2022-63659）。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-2022-63631

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63630
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63647
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63652
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63655
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63658
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63656
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63659

2、IBM 产品安全漏洞

IBM Spectrum Scale 是美国 IBM 公司的一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。该产品支持帮助客户减少存储成本，同时提高云、大数据和分析环境中的安全性和管理效率等。IBM i 是一套运行在 IBM Power Systems 和 IBM PureSystems 中的操作系统。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。IBM Sterling Secure Proxy 是一个用于确保组织非保护区(DMZ)中文件安全传输的应用程序代理。IBM Security Identity Governance and Intelligence（IGI）是的一套身份治理解决方案。该产品包括生命周期管理、访问风险评估和身份认证管理等功能。IBM Robotic Process Automation 是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 InfoSphere Information Server 是一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行未授权访问，在 URL 参数中获取敏感信息，导致拒绝服务，执行任意命令等。

CNVD 收录的相关漏洞包括：IBM i SQL 注入漏洞（CNVD-2022-63180）、IBM Aspera 访问控制错误漏洞、IBM Sterling Secure Proxy 信任管理问题漏洞、IBM Security Identity Governance and Intelligence 信息泄露漏洞（CNVD-2022-63183）、IBM Robotic Process Automation SQL 注入漏洞、IBM InfoSphere Information Server 命令执行漏洞、IBM Sterling External Authentication Server 和 IBM Sterling Secure Proxy 拒绝服务漏洞、IBM Spectrum Scale 加密问题漏洞（CNVD-2022-63371）。其中，“IBM Robotic Process Automation SQL 注入漏洞、IBM InfoSphere Information Server 命令执行漏洞”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-2022-63371
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63180
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63179
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63184
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63183

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63367

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63369

https://www.cnvd.org.cn/flaw/show/CNVD-2022-63373

3、 Siemens 产品安全漏洞

Parasolid 是一种 3D 几何建模工具，支持各种技术，包括实体建模、直接编辑和自由曲面/片材建模。Simcenter Femap 是一种高级仿真应用程序，用于创建、编辑和检查复杂产品或系统的有限元模型。本周，上述产品被披露存在越界写入漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Simcenter Femap and Parasolid 越界写入漏洞（CNVD-2022-62982、CNVD-2022-62980、CNVD-2022-62979、CNVD-2022-62985、CNVD-2022-62984、CNVD-2022-62983、CNVD-2022-62986、CNVD-2022-62990）。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-2022-62982

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62980

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62979

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62985

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62984

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62983

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62986

https://www.cnvd.org.cn/flaw/show/CNVD-2022-62990

4、 SAP 产品安全漏洞

SAP Adaptive Server Enterprise（ASE）是德国思爱普（SAP）公司的一款关系型数据库服务器。SAP Cloud Connector 是一款用于连接 SAP 云平台的连接器。SAP Net Weaver Application Server 是一款应用程序服务器。SAP Mobile Platform 是用于构建和部署移动 app 的便于用户连接的平台。SAP NetWeaver 是一套面向服务的集成化应用平台。该平台可为 SAP 应用提供开发和运行环境。SAP Enterprise Portal 是一个应用软件。一个综合性的集成和应用程序平台，可促进跨组织和技术边界的人员、信息和业务流程的一致性。SAP SAPCAR 是一款用于压缩和/或解压缩 SAP 存档文件的实用程序。SAP Focused Run 是一个数据中心和大客户系统运维管理方案(高容量监控，警报，诊断和分析的终极解决方案)。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证书认证，通过路径遍历进行代码注入从而访问文件或目录，在客户端执行 JavaScript 代码，将自己的权限提升为本地 Unix 系统上的 root 权限等。

CNVD 收录的相关漏洞包括：SAP Adaptive Server Enterprise 权限提升漏洞、SAP Cloud Connector 信任管理问题漏洞、SAP Cloud Connector 路径遍历漏洞、SAP Net

Weaver Application Server 跨站脚本漏洞（CNVD-2022-63625）、SAP Mobile Platform SDK 资源管理错误漏洞、SAP NetWeaver Enterprise Portal 跨站脚本漏洞（CNVD-2022-63628）、SAP SAPCAR 存在输入验证错误漏洞、SAP Focused Run 访问控制错误漏洞。其中，“SAP Adaptive Server Enterprise 权限提升漏洞、SAP SAPCAR 存在输入验证错误漏洞、SAP Focused Run 访问控制错误漏洞”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-2022-63619
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63622
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63626
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63625
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63624
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63628
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63627
https://www.cnvd.org.cn/flaw/show/CNVD-2022-63629

5、Tenda AX12 跨站请求伪造漏洞（CNVD-2022-63551）

Tenda AX12 是中国腾达（Tenda）公司的一款双频千兆 Wifi 6 无线路由器。本周，Tenda AX12 V22.03.01.21_CN 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞伪造恶意请求诱骗受害者点击执行敏感操作。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-2022-63551

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：https://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-2022-62978	Siemens Simcenter Femap and Parasolid 越界读取漏洞（CNVD-2022-62978）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-518824.html
CNVD-2022-62987	Siemens Simcenter Femap and Parasolid 未初始化指针的访问漏洞（CNVD-2022-62987）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-518824.html
CNVD-2022-62991	Siemens Simcenter Femap and Parasolid 越界写入漏洞（CNVD-2022-62991）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-518824.html

CNVD-2022-62995	Siemens Simcenter Femap and Parasolid 越界写入漏洞（CNVD-2022-62995）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-518824.html
CNVD-2022-63000	Siemens Mendix SAML Module 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-638652.html
CNVD-2022-62998	Siemens CoreShield OWG Software 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-589975.html
CNVD-2022-63613	Microsoft Windows TCP/IP 远程代码执行漏洞（CNVD-2022-63613）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34718
CNVD-2022-63617	Microsoft Dynamics CRM 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34700
CNVD-2022-63616	Microsoft Dynamics CRM 远程代码执行漏洞（CNVD-2022-63616）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35805
CNVD-2022-63632	Samsung SMR 空指针解引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=4

小结：本周，Samsung 产品被披露存在多个漏洞，攻击者可利用漏洞启动某些活动，进行越界写入，执行代码等。此外，IBM、Siemens、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞进行未授权访问，绕过证书认证，导致拒绝服务，执行任意命令等。另外，Tenda AX12 V22.03.01.21_CN 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞伪造恶意请求诱骗受害者点击执行敏感操作。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、Social Codia SMS 任意文件上传漏洞

验证描述

Social Codia SMS 是印度 Social Codia 公司的一个库存管理系统。

Social Codia SMS v1.0 版本存在任意文件上传漏洞，攻击者可利用该漏洞通过精心设计的 PHP 文件执行任意代码。

验证信息

POC 链接：https://github.com/D4rkP0w4r/sms-Unrestricted-File-Upload-RCE-POC

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-63534

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. Apple 发布 iOS 和 macOS 更新以修补积极利用的零日漏洞

Apple 发布了另一轮安全更新，以解决 iOS 和 macOS 中的多个漏洞，包括一个新的零日漏洞，该漏洞已在野外攻击中使用。

参考链接：https://thehackernews.com/2022/09/apple-releases-ios-and-macos-updates-to.html

2. 惠普商务设备中的一些固件错误尚未修复

影响多个 HP Enterprise 设备的六个固件错误尚未修复，其中一些自 2021 年 7 月以来就一直存在。

参考链接：https://securityaffairs.co/wordpress/135592/security/firmware-bugs-hp-devices.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