国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 01 月 11 日-2021 年 01 月 17 日　　2021 年第 2 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 566 个，其中高危漏洞 224 个、中危漏洞 294 个、低危漏洞 48 个。漏洞平均分值为 6.03。本周收录的漏洞中，涉及 0day 漏洞 336 个（占 59%），其中互联网上出现“Anchor CMS 'markdown'跨站脚本漏洞、Quixplorer 输入验证错误漏洞”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 4306 个，与上周（3992 个）环比增加 8%。

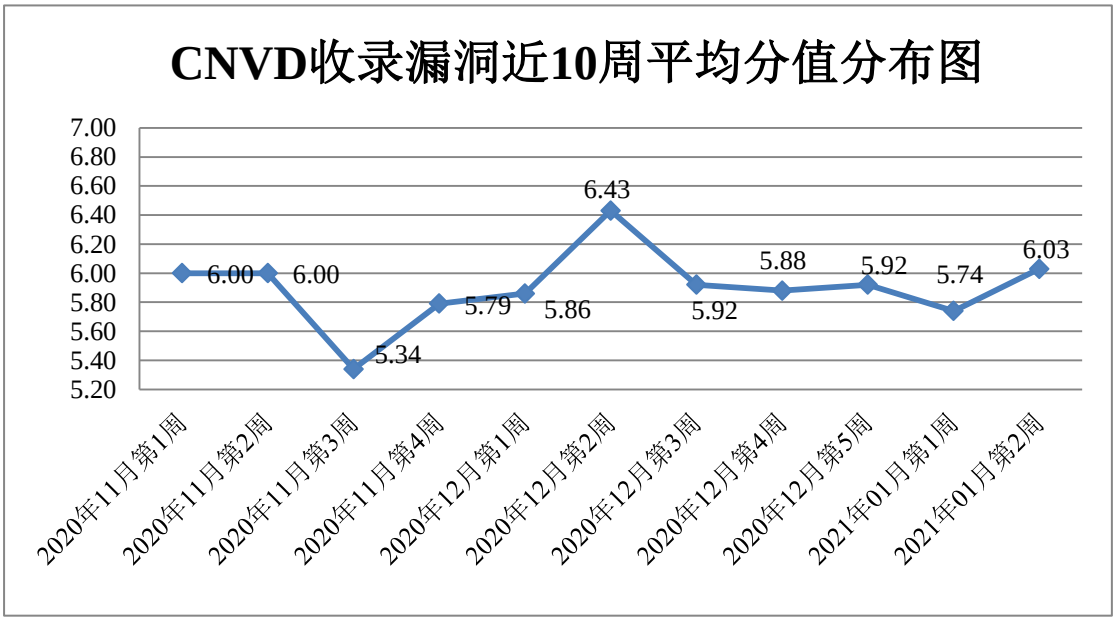

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 23 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 237 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 28 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 29 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：

北京爱奇艺科技有限公司、创维数字股份有限公司、深圳市美科星通信技术有限公司、成都飞鱼星科技股份有限公司、广州虎牙信息科技有限公司、重庆丰圣佳电子商务有限公司、北京致远互联软件股份有限公司、深圳智嵌物联网电子技术有限公司、广州红帆电脑科技有限公司、深圳市吉祥腾达科技有限公司、厦门美图网科技有限公司、友讯电子设备（上海）有限公司、微软(中国)有限公司、深圳市博思协创网络科技有限公司、山西牛酷信息科技有限公司、上海纵之格科技有限公司、深圳艾维信息有限公司、合肥明靖信息科技有限公司、深圳市华德安科技有限公司、深圳市电航科技发展有限公司、深圳市优多贸易有限公司、网易有道信息技术（北京）有限公司、普联技术有限公司、广州网易计算机系统有限公司、思科系统（中国）网络技术有限公司、四方继保自动化股份有限公司、苏州恩斯特网络科技有限公司、南京冠邦网络技术有限责任公司、湖北淘码千维信息科技有限公司、北京华艺汇龙网络科技有限公司、Zoom 视频通讯有限公司、中移物联网有限公司、全讯汇聚网络科技（北京）有限公司、烽火通信科技股份有限公司、江西铭软科技有限公司、吉翁电子（深圳）有限公司、湖南翱云网络科技有限公司、合肥讯飞读写科技有限公司、正方软件股份有限公司、沧州市凡诺广告传媒有限公司、湖南一唯信息科技有限公司、山西沃奇德格科技有限公司、深圳维盟科技股份有限公司、北京三快科技有限公司、鹏为软件股份有限公司、山西先启科技有限公司、北京星网锐捷网络技术有限公司、四川万博教育软件股份有限公司、华硕电脑（上海）有限公司、北京玛格泰克科技发展有限公司、江苏易安联网络技术有限公司、中国招标公共服务平台有限公司、北京中成科信科技发展有限公司、西门子（中国）有限公司、支付宝（中国）网络技术有限公司、苹果电子产品商贸（北京）有限公司、欧姆龙自动化（中国）有限公司、山西龙采科技有限公司、北京中科服科技有限公司、厦门易尔通网络科技有限公司、锐捷网络股份有限公司、深圳市和为顺网络技术有限公司、唐山市柳林自动化设备有限公司、北京金盘鹏图软件技术有限公司、南通百度公司、太仓苏易信息科技有限公司、惠州市敏蝶科技有限公司、北京惠尔阳光健康科技有限责任公司、大唐电信科技股份有限公司、山西龙采科技有限公司阳泉分公司、上海新网程信息技术股份有限公司、昆明云涛科技有限公司、贝尔金国际有限公司、北京国炬信息技术有限公司、广发证券股份有限公司、小米科技有限责任公司、数字天堂(北京)网络技术有限公司、上海宽娱数码科技有限公司、北京中远麒麟科技有限公司、天津神舟通用数据技术有限公司、搜狗公司、华科网络、米酷资源网、京东安全应急响应中心、飞飞影视导航系统、睿谷信息管理系统、米酷影视、VMware 基金会、海洋 CMS、易优 CMS、熊海 cms 、超级 cms 、优艺 cms 、Lantis Project、HeyBBS、libreCMC、ZZCMS、seacms、

yycms、FastAdmin、Lantis1008 和 ucms。

本周，CNVD 发布了《关于致远 OA 系统存在文件上传漏洞的安全公告》、《Microsoft 发布 2021 年 1 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5959

https://www.cnvd.org.cn/webinfo/show/5974

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、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京神州绿盟科技有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、国瑞数码零点实验室、南京众智维信息科技有限公司、北京华云安信息技术有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司、北京顶象技术有限公司、山东华鲁科技发展股份有限公司、安徽长泰信息安全服务有限公司、新疆海狼科技有限公司、河南信安世纪科技有限公司、广州市蓝爵计算机科技有限公司、广西等保安全测评有限公司、京东云安全、北京机沃科技有限公司、北京惠而特科技有限公司、浙江鹏信信息科技股份有限公司、江苏保旺达软件技术有限公司、内蒙古奥创科技有限公司、星云博创科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、山东云安全技术有限公司、百度 AIoT 安全团队、北京信联科汇科技有限公司、上海观安信息技术股份有限公司、信联科技（南京）有限公司、郑州云智信安安全技术有限公司、任子行网络技术股份有限公司、福建省海峡信息技术有限公司、北京安华金和科技有限公司、上海嵴函信息科技有限公司、北京智游网安科技有限公司、北京驭安科技有限公司、联想全球安全实验室、中国科学院计算机网络信息中心、北京时代新威信息技术有限公司、深圳市魔方安全科技有限公司、北京明朝万达科技股份有限公司（安元实验室）、上海市信息安全测评认证中心、北京云科安信科技有限公司（Seraph 安全实验室）及其他个人白帽子向 CNVD 提交了 4306 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 2360 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）	1150	1150
奇安信网神（补天平台）	934	934
北京天融信网络安全技术有限公司	321	6
哈尔滨安天科技集团股份有限公司	289	0

上海交大	276	276
华为技术有限公司	230	0
北京神州绿盟科技有限公司	169	0
新华三技术有限公司	146	0
深信服科技股份有限公司	141	0
中国电信集团系统集成有限责任公司	90	90
北京启明星辰信息安全技术有限公司	58	1
北京数字观星科技有限公司	50	0
中国电信股份有限公司网络安全产品运营中心	20	0
杭州安恒信息技术股份有限公司	16	16
北京知道创宇信息技术股份有限公司	5	0
北京山石网科信息技术有限公司	230	230
国瑞数码零点实验室	180	180
南京众智维信息科技有限公司	119	119
北京华云安信息技术有限公司	74	74
北京天地和兴科技有限公司	44	44
河南灵创电子科技有限公司	36	36
北京顶象技术有限公司	33	33
山东华鲁科技发展股份有限公司	31	31
安徽长泰信息安全服务有限公司	30	30
杭州迪普科技股份有限公司	27	0
新疆海狼科技有限公司	23	23
河南信安世纪科技有限公司	20	20
广州市蓝爵计算机科技有限公司	16	16
广西等保安全测评有限公司	16	16
京东云安全	13	13
北京机沃科技有限公司	11	11
北京惠而特科技有限公司	9	9
浙江鹏信信息科技股份有限公司	9	9
江苏保旺达软件技术有限公司	9	9

内蒙古奥创科技有限公司	7	7
星云博创科技有限公司	7	7
远江盛邦（北京）网络安全科技股份有限公司	6	6
山东云天安全技术有限公司	6	6
百度 AIoT 安全团队	6	6
北京信联科汇科技有限公司	6	6
上海观安信息技术股份有限公司	4	4
信联科技（南京）有限公司	3	3
郑州云智信安安全技术有限公司	3	3
任子行网络技术股份有限公司	2	2
福建省海峡信息技术有限公司	2	2
北京安华金和科技有限公司	2	2
上海峭函信息科技有限公司	2	2
北京华顺信安科技有限公司	1	0
北京智游网安科技有限公司	1	1
北京驭安科技有限公司	1	1
联想全球安全实验室	1	1
中国科学院计算机网络信息中心	1	1
北京时代新威信息技术有限公司	1	1
深圳市魔方安全科技有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
上海市信息安全测评认证中心	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
CNCERT 山西分中心	5	5
CNCERT 四川分中心	3	3
CNCERT 甘肃分中心	1	1
个人	856	856
报送总计	5756	4306

本周漏洞按类型和厂商统计

本周，CNVD 收录了 566 个漏洞。应用程序 293 个，WEB 应用 150 个，网络设备

（交换机、路由器等网络端设备）60 个，智能设备（物联网终端设备）34 个，安全产品 17 个，操作系统 12 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	293
WEB 应用	150
网络设备（交换机、路由器等网络端设备）	60
智能设备（物联网终端设备）	34
安全产品	17
操作系统	12

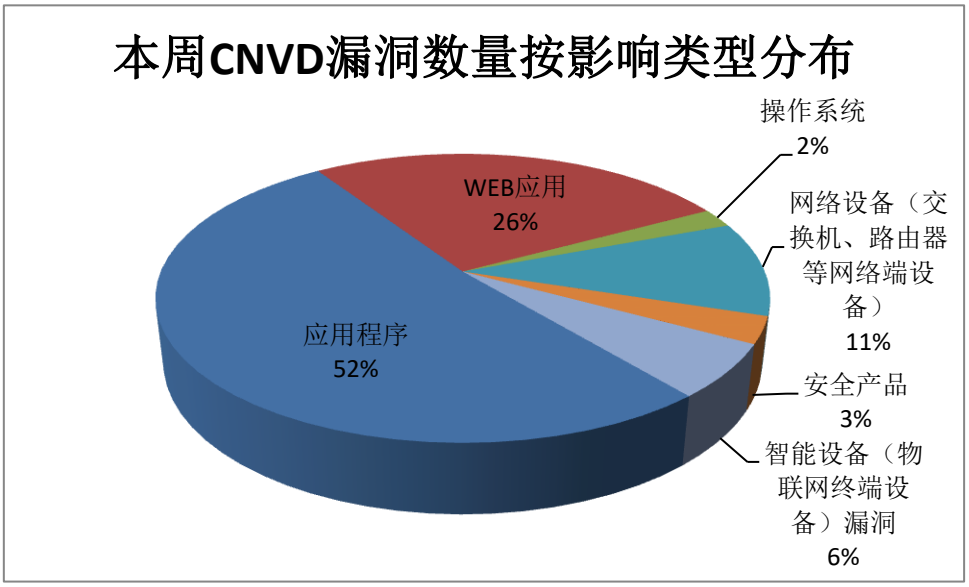

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、北京海腾时代科技有限公司、SIEMENS 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	36	6%
2	北京海腾时代科技有限公司	34	6%
3	SIEMENS	28	5%
4	SEACMS	17	3%
5	SAP	17	3%
6	Dell	14	2%
7	FasterXML	13	2%
8	k7 computing	13	2%
9	Open-Xchange	11	3%
10	其他	383	68%

本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，44 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Scalance X Products 堆缓冲区溢出漏洞、Sonicwall SMA100 操作系统命令注入漏洞、JT2Go and Teamcenter Visualization 堆缓冲区溢出漏洞（CNVD-2021-02577）”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/

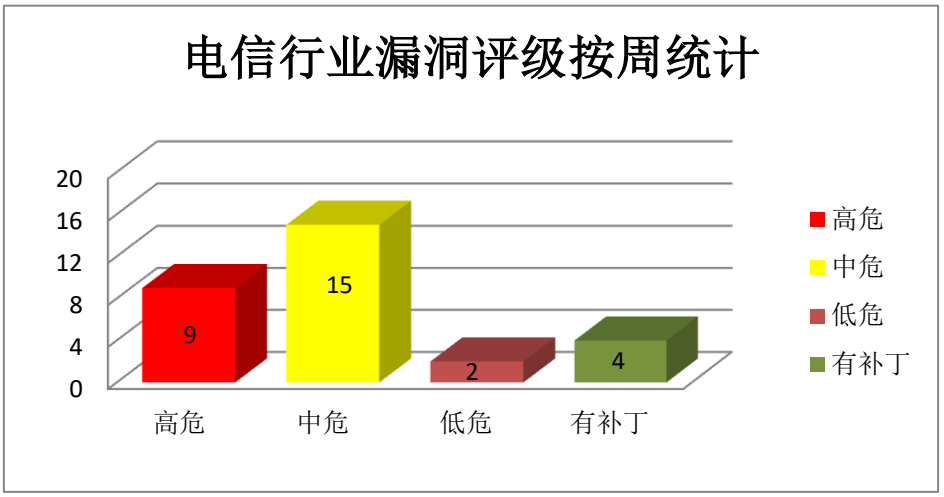

图 3 电信行业漏洞统计

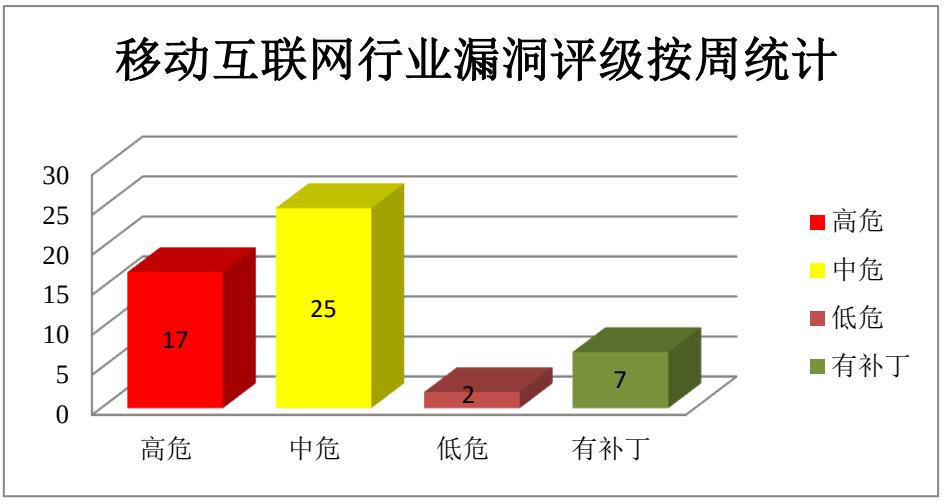

图 4 移动互联网行业漏洞统计

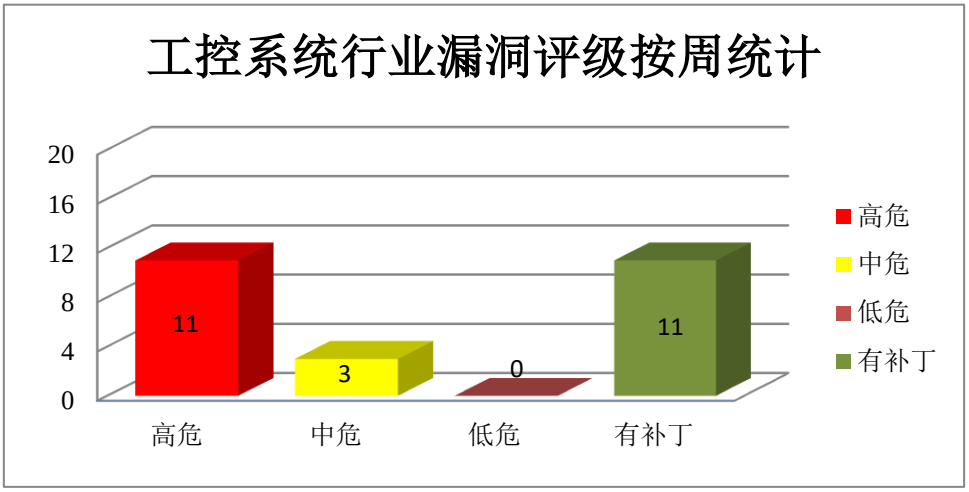

图 5 工控系统行业漏洞统计

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 Sterling B2B Integrator 是一个交易引擎，是一套根据您的业务需求运行您定义和管理的流程的组件。IBM Engineering Workflow Management (EWM)是一款团队协作工具，集成了各种开发任务，包括迭代计划、流程定义、变更管理、缺陷跟踪、源代码控制、构建自动化和报告。IBM Spectrum Protect Plus 是用于虚拟环境的数据保护和可用性解决方案，可在几分钟内完成部署，并在一小时内为您的环境提供保护。IBM Security Guardium Insights 是一个现代化的混合云数据安全中心，旨在提供有关组织数据安全性和合规性状况的可靠视图。IBM Workload Automation 是一款用于批处理和实时工作负载管理的软件。IBM Security Guardium Data Encryption (GDE)提供了一组模块化的加密解决方案，可帮助安全团队有效地实现整个组织的静态数据安全性。本周，上述产品被披露存在信息泄露和任意代码执行漏洞，攻击者可利用漏洞获取敏感信息，以 SYSTEM 权限执行任意代码。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 任意代码执行漏洞、IBM Engineering Workflow Management 信息泄露漏洞、IBM Spectrum Protect Plus 信息泄露漏洞（CNVD-2021-03029）、IBM Security Guardium Insights 信息泄露漏洞（CNVD-2021-03529、CNVD-2021-03528、CNVD-2021-03530）、IBM Workload Automation 信息泄露漏洞（CNVD-2021-03552）、IBM Security Guardium Data Encryption 信息泄露漏洞。其中，“IBM Sterling B2B Integrator 任意代码执行漏洞”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-2021-02005

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03013

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03029

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03529

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03528

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03530

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03552

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03559

2、Dell 产品安全漏洞

Dell Inspiron 5675 BIOS 是一个可为设备提供基本输入输出、开机后自检和系统自启动功能的程序。Dell EMC PowerStore 是一款存储设备。Dell Encryption 是一套数据保护解决方案。Dell Endpoint Security Suite 是一套网络安全套件。Dell Inspiron 7352 BIOS 是一款系统更新驱动程序。Dell EMC Avamar Server 是美国戴尔（DELL）公司的一套用于服务器的完全虚拟化的备份和恢复软件。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提升的权限，导致某些用户凭证的泄露，执行任意代码等。

CNVD 收录的相关漏洞包括：Dell Inspiron 5675 BIOS 访问控制错误漏洞、Dell EMC PowerStore 信息泄露漏洞、Dell Encryption 和 Dell Endpoint Security Suite 提权漏洞、Dell Inspiron 7352 BIOS 引导服务覆盖漏洞、Dell Inspiron 7347 BIOS 引导服务覆盖漏洞、Dell EMC PowerStore 访问控制错误漏洞、Dell EMC Avamar Server SQL 注入漏洞、Dell EMC Avamar Server 路径遍历漏洞。其中，除“Dell EMC PowerStore 信息泄露漏洞、Dell EMC PowerStore 访问控制错误漏洞”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-2021-02357

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02359

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03011

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03010

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03009

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03038

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03541

https://www.cnvd.org.cn/flaw/show/CNVD-2021-03547

3、Adobe 产品安全漏洞

Adobe Bridge 是一款免费数字资产管理应用程序。Adobe InCopy 是 Adobe 公司推出的专业文字处理程序，与 Adobe InDesign 集成在一起。Adobe Bridge 是一款免费数字资产管理应用程序。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。Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图

像处理软件。Adobe Illustrator 2020 是一款矢量图编辑器。Adobe Animate 是一款多媒体创作和计算机动画程序。Adobe Campaign Classic（ACC）是一套跨渠道客户体验营销平台。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，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Bridge 越界写入漏洞（CNVD-2021-02367）、Adobe InCopy 不受控搜索路径元素漏洞、Adobe Bridge 越界写入漏洞（CNVD-2021-02368）、Adobe Acrobat 和 Reader 信息泄露漏洞（CNVD-2021-02375）、Adobe Photoshop 堆缓冲区溢出漏洞、Adobe Illustrator 2020 不受控搜索路径元素漏洞、Adobe Animate 不受控搜索路径元素漏洞、Adobe Campaign Classic 服务器端请求伪造漏洞。其中，除“Adobe Acrobat 和 Reader 信息泄露漏洞（CNVD-2021-02375）”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-2021-02367
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02370
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02368
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02375
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02374
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02373
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02372
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02371

4、Siemens 产品安全漏洞

JT2Go 是一个 3D JT 查看工具，允许用户查看 JT，PDF，Solid Edge，PLM XML 与现有的 JT，VFZ、CGM、TIF 数据。Teamcenter 可视化软件使企业能够增强他们的产品生命周期管理(PLM)环境，该软件使企业用户能够在单一环境中访问文档、2D 图纸和 3D 模型。SCALANCE X 是一个开关用于连接工业部件，例如：可编程逻辑控制器(plc)或人机界面(HMIs)。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：JT2Go and Teamcenter Visualization 堆栈缓冲区溢出漏洞（CNVD-2021-02579、CNVD-2021-02578）、JT2Go and Teamcenter Visualization 堆缓冲区溢出漏洞（CNVD-2021-02577、CNVD-2021-02584、CNVD-2021-02582、CNVD-2021-02586、CNVD-2021-02585）、Scalance X Products 堆缓冲区溢出漏洞。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-2021-02579
https://www.cnvd.org.cn/flaw/show/CNVD-2021-02578

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02577

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02584

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02582

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02586

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02585

https://www.cnvd.org.cn/flaw/show/CNVD-2021-02595

5、Belkin LINKSYS RE6500 拒绝服务漏洞

Linksys RE6500 是 Belkin 推出的一款 AC1200 双频 WiFi 扩展器。本周，Belkin LINKSYS RE6500 被披露存在拒绝服务漏洞。攻击者可通过长/goform/langSwitch langSelectionOnly 参数利用该漏洞导致拒绝服务。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-2021-03365

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-2021-02031	OIC Exponent CMS 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/exponentcms/exponent-cms/commit/a8efd9ca71fc9b8b843ad0910d435d237482ee31
CNVD-2021-02036	ISPConfig SQL 注入漏洞（CNVD-2021-02036）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ispconfig.org/blog/ispconfig-3-2-2-released-important-security-update/
CNVD-2021-02594	Scalance X Products 堆缓冲区溢出漏洞（CNVD-2021-02594）	高	厂商已发布相关漏洞补丁链接，请及时更新：https://cert-portal.siemens.com/productcert/pdf/ssa-139628.pdf
CNVD-2021-02817	K7 Computing K7AntiVirus Premium 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://support.k7computing.com/index.php?/selfhelp/view-article/Advisory-issued-on-6th-January-2021
CNVD-2021-02823	Palo Alto Networks Cortex XDR Agent 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.paloaltonetworks.com/CVE-2020-2049

CNVD-2021-03000	Sonicwall SMA100 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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0022
CNVD-2021-03019	Nvidia GPU Display Driver 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nvidia.custhelp.com/app/answers/detail/a_id/5142
CNVD-2021-03260	D-Link DAP-1650 验证绕过漏洞	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.dlink.com/en/consumer
CNVD-2021-03374	TerraMaster TOS 远程命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://terramaster.com/
CNVD-2021-03551	Juniper Networks Junos OS 权限提升漏洞（CNVD-2021-03551）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.juniper.net/InfoCenter/index?page=content&id;=JSA11100&actp;=METADATA

小结：本周，IBM 产品被披露存在信息泄露和任意代码执行漏洞，攻击者可利用漏洞获取敏感信息，以 SYSTEM 权限执行任意代码。此外，Dell、Adobe、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取提升的权限，导致某些用户凭证的泄露，执行任意代码，造成拒绝服务等。另外，Belkin LINKSYS RE6500 被披露存在拒绝服务漏洞。攻击者可通过长/goform/langSwitch langSelectionOnly 参数利用该漏洞导致拒绝服务。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、Anchor CMS 'markdown'跨站脚本漏洞

验证描述

Anchor CMS 是一个轻量级 CMS 建站系统。

Anchor CMS 'markdown'存在跨站脚本漏洞，攻击者可利用漏洞获取用户 cookie 等敏感信。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49403

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-03539

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. 新西兰央行称其数据系统遭黑客攻击，或已获取商业和个人敏感信息

新西兰央行上周日表示，该行的一个数据系统已被一名身份不明的黑客入侵，该黑客有可能已经获取商业和个人敏感信息。这家总部位于惠灵顿的银行在一份声明中说，新西兰储备银行用于共享和存储敏感信息的第三方文件共享服务已被非法访问。

参考链接：https://www.cnbeta.com/articles/tech/1076163.htm

2. 安全研究人员获取 Parler 社交网络 70TB 用户数据

该社交网络因被用于暴动者策划上周的国会入侵活动，而被大量人员进行数据搜刮。70TB 的数据包括用户个人资料、视频、照片、发贴内容等。据称，这些都是 Parler 的公开数据。

参考链接：https://cybernews.com/news/70tb-of-parler-users-messages-videos-and-posts-leaked-by-security-researchers/

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