国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 05 月 31 日-2021 年 06 月 06 日　　2021 年第 22 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 600 个，其中高危漏洞 158 个、中危漏洞 383 个、低危漏洞 59 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 308 个（占 51%），其中互联网上出现“Sourcecodesterk Doctor Appointment System 跨站脚本漏洞、pczupil X2CRM 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 3759 个，与上周（2984 个）环比增加 26%。

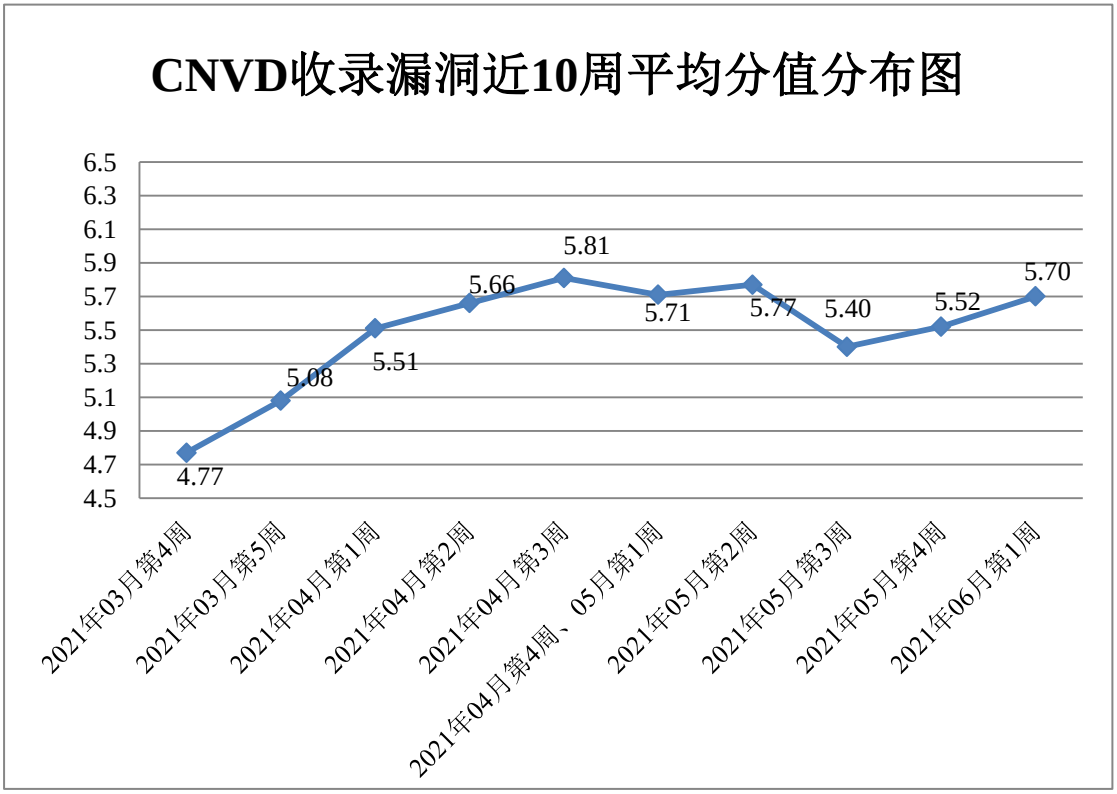

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 起，向基础电信企业通报漏洞事件 9 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 323 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 32 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 47 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、淄博闪灵网络科技有限公司、众勤通信设备贸易（上海）有限公司、中控智慧科技股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、正方软件股份有限公司、浙江零跑科技有限公司、长沙米拓信息技术有限公司、运城市盘石网络科技有限公司、用友网络科技股份有限公司、英诺激光科技股份有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新华新媒文化传播有限公司、武汉东信同邦信息技术有限公司、潍坊家园驿站电子技术有限公司、微宏软件技术（杭州）有限公司、统信软件技术有限公司、泰安梦泰尔软件有限公司、太原扁舟科技有限责任公司、苏州万户网络科技有限公司、四平市九州易通科技有限公司、石家庄市征红网络科技有限公司、施耐德电气（中国）有限公司、深圳维盟科技股份有限公司、深圳市中科网威科技有限公司、深圳市鑫塔科技有限公司、深圳市微耕实业有限公司、深圳市网域科技技术有限公司、深圳市深海捷科技有限公司、深圳市锐明技术股份有限公司、深圳市魔球科技有限公司、深圳市联天通信技术有限公司、深圳市吉祥腾达科技有限公司、深圳市博克时代科技开发有限公司、深圳品誉实业有限公司、深圳警翼智能科技股份有限公司、深圳华域数安科技有限公司、深圳奥联信息安全技术有限公司、上海建文软件科技有限公司、上海达策信息技术有限公司、上海博达数据通信有限公司、熵基科技股份有限公司、任子行网络技术股份有限公司、全讯汇聚网络科技（北京）有限公司、鹏为软件股份有限公司、宁波痘鱼网络有限公司、美国菲力尔公司、联想集团、蓝网科技股份有限公司、江西金磊科技发展有限公司、江苏邦宁科技有限公司、建文软件科技有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、杭州图特信息科技有限公司、杭州海康威视数字技术股份有限公司、杭州艾朴软件有限公司、海南赞赞网络科技有限公司、海口易讯天空信息技术有限公司、桂林崇胜网络科技有限公司、广州图创计算机软件开发有限公司、广州同聚成电子科技有限公司、广西天手网络科技有限公司、富士胶片（中国）投资有限公司、帆软软件有限公司、东莞市同享软件科技有限公司、戴尔（中国）有限公司、成都星锐蓝海网络科技有限公司、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、北京中成科信科技发展有限公司、北京原创先锋网络科技发展有限公司、北京星网锐捷网络技术有限公司、北京神州数码云科信息技术有限公司、北京灵州网络技术有限公司、北京金和网络股份有限公司、北京和利时集团、北京多点在线科技有限公司、北京博乐虎科技有

限公司、北京碧海威科技有限公司、北京百卓网络技术有限公司、北京百容千域软件技术开发有限责任公司、北京爱奇艺科技有限公司、安徽富煌科技有限公司、里客云科技、鱼跃 CMS、狂雨小说 cms、OPPO 安全应急响应中心、Zzcms、SEACMS、Redis、Pluck CMS、MacCMS、Lexmark、General Mobile、Emlog 和 DiYunCMS。

本周，CNVD 发布了《关于用友 NC BeanShell 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6491

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京神州绿盟科技有限公司、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、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。广州易东信息安全技术有限公司、南京众智维信息科技有限公司、北京山石网科信息技术有限公司、北京信联科汇科技有限公司、河南信安世纪科技有限公司、湖北珞格科技发展有限公司、河南灵创电子科技有限公司、北京天地和兴科技有限公司、山东云天安全技术有限公司、新疆海狼科技有限公司、山东新潮信息技术有限公司、杭州木链物联网科技有限公司、北京安帝科技有限公司、江西省掌控者信息安全技术有限公司、浙江大学控制科学与工程学院、浙江御安信息技术有限公司、郑州赛欧思科技有限公司、广州百蕴启辰科技有限公司、武汉绿色网络信息服务有限责任公司、北京机沃科技有限公司、北京时代新威信息技术有限公司、北京远禾科技有限公司、博智安全科技股份有限公司、广州安亿信软件科技有限公司、贵州多彩宝互联网服务有限公司、杭州美创科技有限公司、江苏晟晖信息科技有限公司、山东云天安全大数据技术有限公司、上海上讯信息技术股份有限公司、深圳市魔方安全科技有限公司及其他个人白帽子向 CNVD 提交了 3759 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 2196 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）	957	957
奇安信网神（补天平台）	658	658
上海交大	581	581
哈尔滨安天科技集团股份有限公司	311	0
北京神州绿盟科技有限公司	211	12

深信服科技股份有限公司	152	1
北京天融信网络安全技术有限公司	151	1
北京数字观星科技有限公司	115	0
北京启明星辰信息安全技术有限公司	115	7
华为技术有限公司	107	0
新华三技术有限公司	103	0
恒安嘉新（北京）科技股份公司	92	0
天津市国瑞数码安全系统股份有限公司	28	0
卫士通信息产业股份有限公司	20	0
远江盛邦（北京）网络安全科技股份有限公司	10	10
内蒙古奥创科技有限公司	10	10
北京知道创宇信息技术股份有限公司	5	0
广州易东信息安全技术有限公司	322	322
南京众智维信息科技有限公司	114	114
北京山石网科信息技术有限公司	72	72
北京信联科汇科技有限公司	63	63
河南信安世纪科技有限公司	49	49
湖北珞格科技发展有限公司	29	29
河南灵创电子科技有限公司	21	21
中国电信股份有限公司网络安全产品运营中心	21	0
北京天地和兴科技有限公司	17	17
山东云天安全技术有	16	16

限公司		
新疆海狼科技有限公司	9	9
山东新潮信息技术有限公司	7	7
杭州木链物联网科技有限公司	5	5
北京安帝科技有限公司	4	4
江西省掌控者信息安全技术有限公司	4	4
浙江大学控制科学与工程学院	3	3
浙江御安信息技术有限公司	3	3
郑州赛欧思科技有限公司	3	3
广州百蕴启辰科技有限公司	2	2
武汉绿色网络信息服务有限责任公司	2	2
北京机沃科技有限公司	1	1
北京时代新威信息技术有限公司	1	1
北京远禾科技有限公司	1	1
博智安全科技股份有限公司	1	1
广州安亿信软件科技有限公司	1	1
贵州多彩宝互联网服务有限公司	1	1
杭州美创科技有限公司	1	1
江苏晟晖信息科技有限公司	1	1
山东云天安全大数据技术有限公司	1	1
上海上讯信息技术股份有限公司	1	1
深圳市魔方安全科技有限公司	1	1

西门子（中国）有限公司	1	0
CNCERT 海南分中心	5	5
CNCERT 河北分中心	1	1
CNCERT 青海分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	758	758
报送总计	5170	3759

本周漏洞按类型和厂商统计

本周，CNVD 收录了 600 个漏洞。应用程序 293 个，WEB 应用 197 个，网络设备（交换机、路由器等网络端设备）79 个，操作系统 16 个，安全产品 11 个，智能设备（物联网终端设备）3 个，数据库 1 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	197
网络设备（交换机、路由器等网络端设备）	79
操作系统	16
安全产品	11
智能设备（物联网终端设备）	3
数据库	1

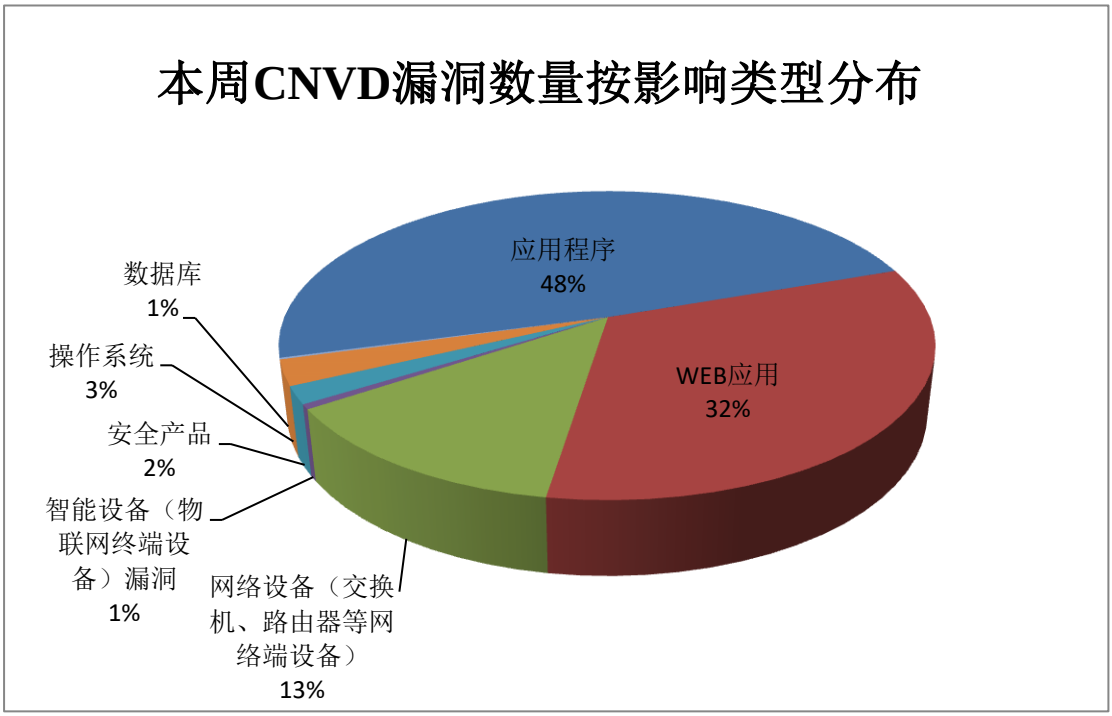

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、SEMCMS、FFmpeg 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	26	4%
2	SEMCMS	25	4%
3	FFmpeg	21	4%
4	ASUS	14	2%
5	Cesanta	12	2%
6	Microsoft	12	2%
7	Qemu	12	2%
8	Mozilla	11	2%
9	HUAWEI	11	2%
10	其他	456	76%

本周行业漏洞收录情况

本周，CNVD 收录了 38 个电信行业漏洞，17 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“Siemens SIMATIC S7-1200 和 S7-1500 CPU 系列内存保护绕过漏洞、Schneider Electric spaceLYnk OS 命令注入漏洞”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/

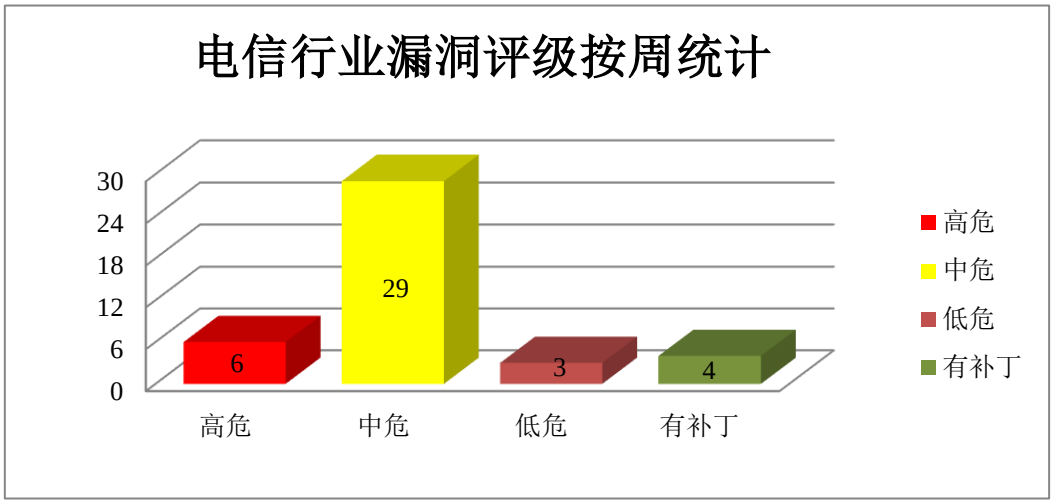

图 3 电信行业漏洞统计

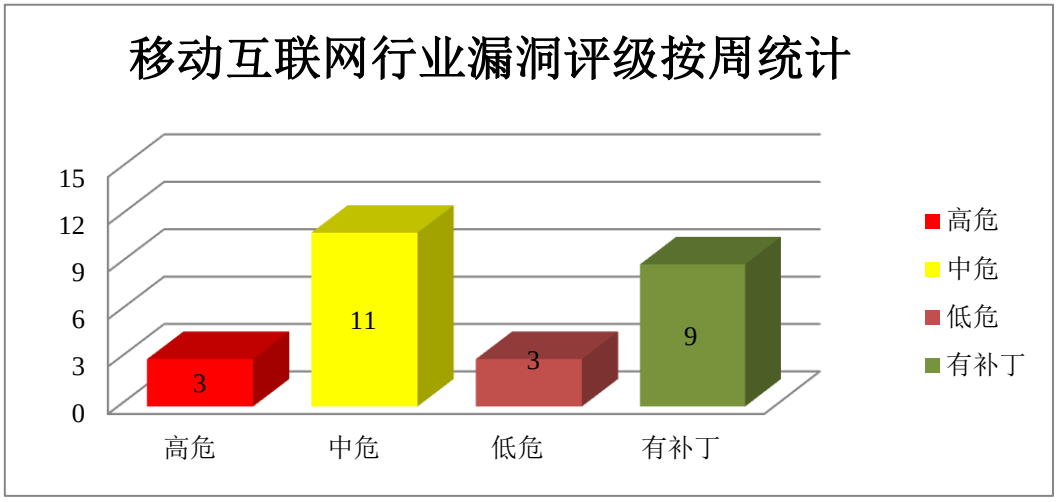

图 4 移动互联网行业漏洞统计

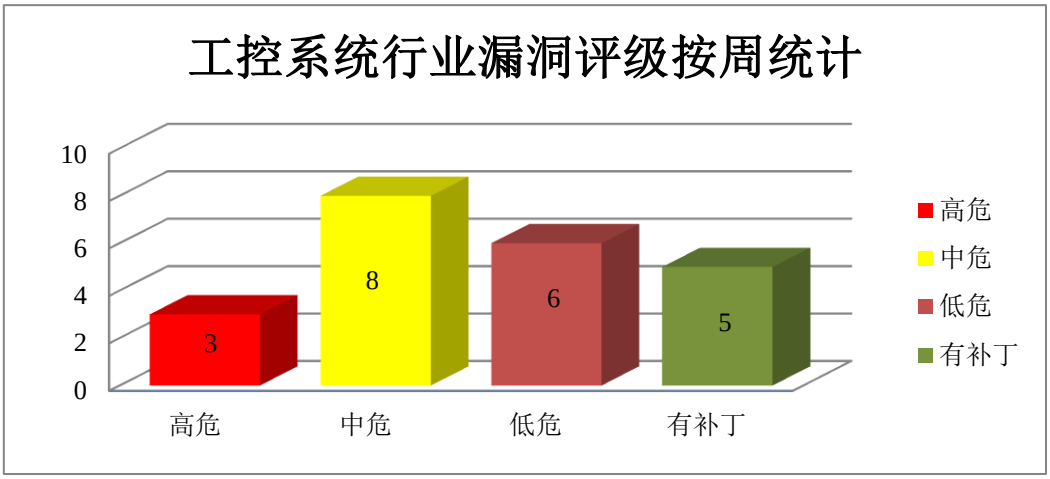

图 5 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Apache Superset up 是美国 （Apache）公司的一个提供大型分布式环境中横向扩展设计应用软件。Apache Ozone 是一个面向 Hadoop 和云原生环境的可伸缩，冗余和分布式对象存储。Apache Tapestry 是一款使用 Java 语言编写的 Web 应用程序框架。Apache OFBiz 是一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache Dubbo 是一款基于 Java 的高性能开源 RPC 框架。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，创建一个可能是恶意的外部 URL，使用特殊构造的 URL 下载 WEB-INF 中的文件等。

CNVD 收录的相关漏洞包括：Apache Ozone 授权问题漏洞、Apache Superset 输入验证错误漏洞、Apache Tapestry 信息泄露漏洞、Apache Tapestry 反序列化漏洞、Apache OFBiz 代码问题漏洞、Apache OFBiz 远程代码执行漏洞、Apache Dubbo 任意代码执行漏洞、Apache Dubbo 反序列化漏洞（CNVD-2021-39669）。其中，除“Apache Ozone 授权问题漏洞、Apache Superset 输入验证错误漏洞、Apache Tapestry 信息泄露漏洞”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-2021-38304

https://www.cnvd.org.cn/flaw/show/CNVD-2021-38303

https://www.cnvd.org.cn/flaw/show/CNVD-2021-38302

https://www.cnvd.org.cn/flaw/show/CNVD-2021-38301

https://www.cnvd.org.cn/flaw/show/CNVD-2021-38305

https://www.cnvd.org.cn/flaw/show/CNVD-2021-38782

https://www.cnvd.org.cn/flaw/show/CNVD-2021-39670

https://www.cnvd.org.cn/flaw/show/CNVD-2021-39669

2、IBM 产品安全漏洞

IBM Cognos Analytics 是美国 IBM 公司的一套商业智能软件。IBM Spectrum Scale 是一套基于 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。IBM Security Verify Access 是一款提高用户访问安全的服务。IBM WebSphere Exteme Scale 是一个弹性的，高度可扩展的内存数据网格。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，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Cognos Analytics XML 外部实体注入漏洞（CNVD-2021-38673）、IBM Cognos Analytics 信息泄露漏洞（CNVD-2021-38672）、IBM

Cognos Analytics 命令执行漏洞、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2021-38670）、IBM Spectrum Scale 权限提升漏洞（CNVD-2021-38676）、IBM Security Verify Access 缓冲区溢出漏洞、IBM WebSphere eXtreme Scale 信息泄露漏洞（CNVD-2021-39041）、IBM Engineering Systems Design Rhapsody 访问控制错误漏洞。其中，除“IBM Cognos Analytics 信息泄露漏洞（CNVD-2021-38672）、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2021-38670）”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-2021-38673
https://www.cnvd.org.cn/flaw/show/CNVD-2021-38672
https://www.cnvd.org.cn/flaw/show/CNVD-2021-38671
https://www.cnvd.org.cn/flaw/show/CNVD-2021-38670
https://www.cnvd.org.cn/flaw/show/CNVD-2021-38676
https://www.cnvd.org.cn/flaw/show/CNVD-2021-38675
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39041
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39675

3、Microsoft 产品安全漏洞

Microsoft Excel 是 Microsoft 公司的办公软件 Microsoft office 的组件之一，是一款电子表格程序。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞实现远程代码执行。

CNVD 收录的相关漏洞包括：Microsoft Excel 远程代码执行漏洞（CNVD-2021-39509、CNVD-2021-39508、CNVD-2021-39512、CNVD-2021-39511、CNVD-2021-39510、CNVD-2021-39516、CNVD-2021-39515、CNVD-2021-39517）。其中，除“Microsoft Excel 远程代码执行漏洞（CNVD-2021-39515）”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-2021-39509
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39508
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39512
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39511
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39510
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39516
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39515
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39517

4、ASUS 产品安全漏洞

ASUS BMC Firmware 是中国华硕（ASUS）公司的一个固件。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞终止 Web 服务。

CNVD 收录的相关漏洞包括：ASUS BMC Firmware 缓冲区溢出漏洞（CNVD-2021-39576、CNVD-2021-39575、CNVD-2021-39578、CNVD-2021-39577、CNVD-2021-39580、CNVD-2021-39579、CNVD-2021-39582、CNVD-2021-39581）。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-2021-39576
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39575
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39578
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39577
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39580
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39579
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39582
https://www.cnvd.org.cn/flaw/show/CNVD-2021-39581

5、Red Hat Ansible 信息泄露漏洞（CNVD-2021-39044）

Red Hat Ansible 是美国红帽（Red Hat）公司的一款计算机系统配置管理器。该产品可用于发布、管理和编排计算机系统。Ansible Tower 是其中的一个提供了用户界面（UI）、仪表板和 REST API 的任务控制应用程序。本周，Red Hat Ansible Tower 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取受影响组件敏感信息。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-2021-39044

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-2021-37943	Emerson Rosemount X-STREAM Gas Analyzer 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新 https://www.emerson.com/en-us/support/security-notifications
CNVD-2021-39028	Synology Download Station 服务器端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/advisory/Synology_SA_21_04
CNVD-2021-39034	Aruba Networks ClearPass Policy Manager 访问控制错误	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

	漏洞		https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-005.txt
CNVD-2021-39045	Linux kernel 缓冲区溢出漏洞（CNVD-2021-39045）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openwall.com/lists/oss-security/2021/05/27/1
CNVD-2021-39257	Mozilla Firefox 拒绝服务漏洞（CNVD-2021-39257）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/
CNVD-2021-39502	Synology Photo Station 路径遍历漏洞（CNVD-2021-39502）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.com/security/advisory/Synology_SA_20_20
CNVD-2021-39506	Mcafee Database Security Server 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kc.mcafee.com/corporate/index?page=content&id=SB10359
CNVD-2021-39543	TIBCO Software Managed File Transfer Command Center 和 Internet Server 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tibco.com/support/advisories/2020/06/tibco-security-advisory-june-30-2020-tibco-managed-file-transfer-2020-9414
CNVD-2021-39550	Samsung SMR 缓冲区溢出漏洞	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.samsungmobile.com/
CNVD-2021-39689	FortiWeb OS 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://www.fortiguard.com/psirt/FG-IR-20-120

小结：本周，Apache 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，创建一个可能是恶意的外部 URL，使用特殊构造的 URL 下载 WEB-INF 中的文件等。此外，IBM、Microsoft、ASUS 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，提升权限，执行任意代码、终止 Web 服务等。另外，Red Hat Ansible Tower 被披露存在信息泄露漏洞。攻击者可利用漏洞获取受影响组件敏感信息。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、Sourcecodesterk Doctor Appointment System 跨站脚本漏洞

验证描述

Sourcecodesterk Doctor Appointment System 是 Sourcecodesterk 开源的一个应用软件。提供了一个预约功能。

Sourcecodesterk Doctor Appointment System 1.0 中的 contactus.php 存在跨站脚本漏洞，远程攻击者可通过 comment 参数利用该漏洞注入任意 Web 脚本或 HTML。

验证信息

POC 链接：https://packetstormsecurity.com/files/161574/Doctor-Appointment-System-1.0-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-39650

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. WordPress 强制对使用 Jetpack 插件的网站执行安全更新

WordPress 强制对五百多万使用 Jetpack 插件的网站执行安全更新。Jetpack 是一个非常受欢迎的 WordPres 插件，提供了免费的安全、性能和管理功能，包括暴力破解保护、网站备份、安全登陆、恶意程序扫描等。

参考链接：https://www.solidot.org/story?sid=67958

2. CODESYS 工业自动化软件被发现 10 个严重漏洞

网络安全研究人员 6 月 3 日披露了多达 10 个影响 CODESYS 自动化软件的关键漏洞，这些漏洞可被利用在可编程逻辑控制器（PLC）上远程执行代码。

参考链接：https://thehackernews.com/2021/06/10-critical-flaws-found-in-codesys.html?&web_view=true

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