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 18 日-2021 年 01 月 24 日　　2021 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 378 个，其中高危漏洞 94 个、中危漏洞 247 个、低危漏洞 37 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 140 个（占 37%），其中互联网上出现“JIZHICMS 跨站脚本漏洞、ZZCMS SQL 注入漏洞（CNVD-2021-04410）”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 6101 个，与上周（4306 个）环比增加 42%。

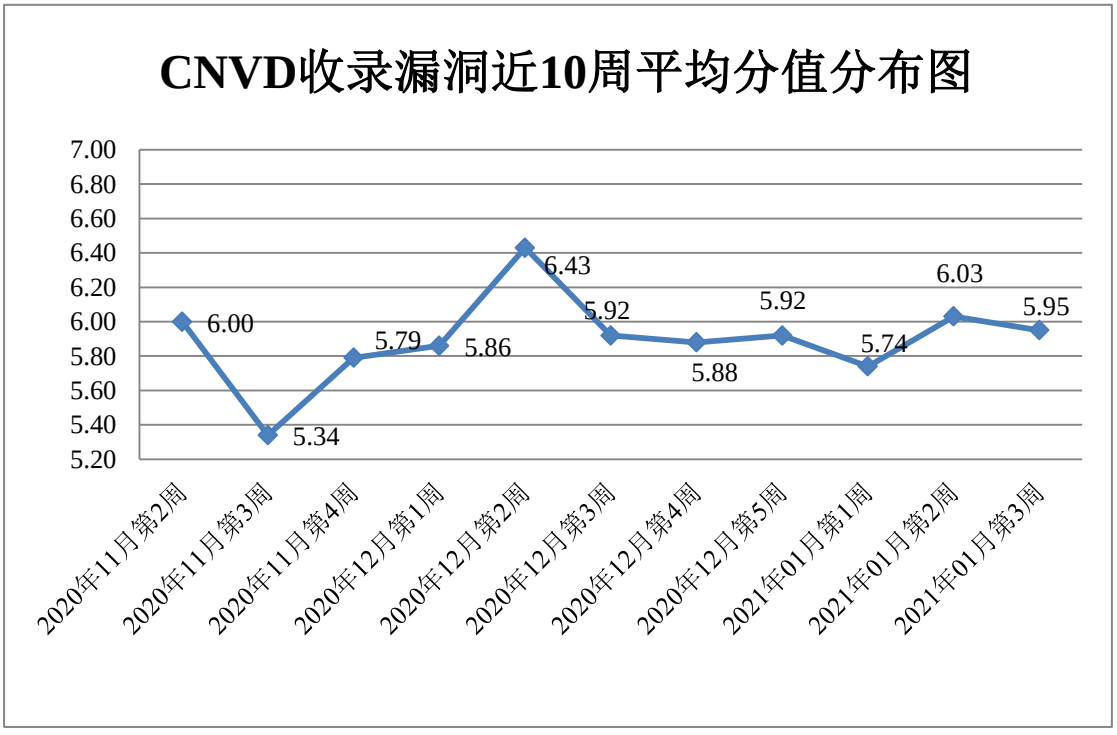

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 起，向基础电信企业通报漏洞事件 8 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 327 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 63 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 38 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：

南宁市烟寒网络科技有限公司、北京因酷时代科技有限公司、杭州乐邦科技有限公司、江苏固德威电源科技股份有限公司、深圳市千寻网络技术有限公司、哈尔滨伟成科技有限公司、上海牛之云网络科技有限公司、北京百度网讯科技有限公司、深圳市博思协创网络科技有限公司、北京熊宝贝科技发展有限公司、锐捷网络股份有限公司、北京金和网络股份有限公司、北京飞书科技有限公司、青岛东胜伟业软件科技有限公司、上海去动网络科技有限公司、北京金山数字娱乐科技有限公司、北京天学网教育科技股份有限公司、武汉小咪网络科技有限公司、普联技术有限公司、北京通达信科科技有限公司、上海熙讯电子科技有限公司、上海拉扎斯信息科技有限公司、成都飞鱼星科技股份有限公司、全讯汇聚网络科技（北京）有限公司、南充市老虎云网络技术有限公司、湖南菠萝互娱网络信息有限公司、上海畅指网络科技有限公司、西门子（中国）有限公司、Zoom 视频通讯有限公司、微软(中国)有限公司、苏州恩斯特网络科技有限公司、谷歌公司、太原迅易科技有限公司、武汉达梦数据库有限公司、北京指掌易科技有限公司、青岛东胜伟业软件有限公司、东莞市千度网络科技有限公司、深圳市圆梦云科技有限公司、湖北淘码千维信息科技有限公司、北京映翰通网络技术股份有限公司、西安昊博智能科技公司、成都奇鲁科技有限公司、湖南一唯信息科技有限公司、上海纵之格科技有限公司、北京三快科技有限公司、广东一一五科技股份有限公司、上海泛微网络科技股份有限公司、北京中成科信科技发展有限公司、厦门快普信息技术有限公司、北京海腾时代科技有限公司、北京搜狗信息服务有限公司、深圳市双梦科技有限公司、台达电子企业管理(上海)有限公司、厦门科拓通讯技术股份有限公司、上海宽娱数码科技有限公司、深圳点猫科技有限公司 、成都不亦说乎科技有限公司、南昌北创科技发展有限公司、深圳维盟科技股份有限公司、杭州恩软信息技术有限公司、南京九则软件科技有限公司、上海商派网络科技有限公司、珠海金山办公软件有限公司、浙江易舸软件有限公司、苏州开心盒子软件有限公司、北京信诺瑞得软件系统有限公司、友讯电子设备（上海）有限公司、昆明云涛科技有限公司、淄博闪灵网络科技有限公司、深圳市辣妈帮科技有限公司、无锡信捷电气股份有限公司、三菱电机（中国）有限公司、研华科技（中国）有限公司、米酷资源网、华科网络、佳佳软件、发货 100、优艺 CMS、熊海 CMS、HeyBBS、UCMS、Weintek、wdja 和 Schneider Electric。

本周，CNVD 发布了《Oracle 发布 2021 年 1 月的安全公告》。详情参见 CNVD 网

站公告内容。

https://www.cnvd.org.cn/webinfo/show/5989

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。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、国瑞数码零点实验室、新疆海狼科技有限公司、上海犀点意象网络科技有限公司、河南信安世纪科技有限公司、山东新潮信息技术有限公司、北京天地和兴科技有限公司、江苏保旺达软件技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、山东华鲁科技发展股份有限公司、河南灵创电子科技有限公司、西安交大捷普网络科技有限公司、安徽长泰信息安全服务有限公司、任子行网络技术股份有限公司、内蒙古奥创科技有限公司、山东云天安全技术有限公司、北京中科微澜科技有限公司、重庆贝特计算机系统工程有限公司、北京华顺信安科技有限公司、北京顶象技术有限公司、北京信联科汇科技有限公司、吉林谛听信息技术有限公司、京东云安全、木链科技、上海市信息安全测评认证中心、北京机沃科技有限公司、广州市蓝爵计算机科技有限公司、四川哨兵信息科技有限公司、北京惠而特科技有限公司、北京圣博润高新技术股份有限公司、北京长亭科技有限公司、上海观安信息技术股份有限公司、武汉明嘉信信息安全检测评估有限公司、北京明朝万达科技股份有限公司、湖南浩基信息技术有限公司、北京时代新威信息技术有限公司、北京智游网安科技有限公司、平安银河实验室、上海峭函信息科技有限公司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）	2872	2872
奇安信网神（补天平台）	760	760
上海交大	431	431
北京天融信网络安全技术有限公司	352	18
哈尔滨安天科技集团股份有限公司	243	0
华为技术有限公司	211	0
北京神州绿盟科技有限公司	146	33
新华三技术有限公司	94	0
深信服科技股份有限公司	90	0

北京启明星辰信息安全技术有限公司	85	16
北京数字观星科技有限公司	50	0
中国电信集团系统集成有限责任公司	35	35
西安四叶草信息技术有限公司	26	26
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
恒安嘉新(北京)科技股份公司	5	3
北京知道创宇信息技术股份有限公司	2	0
阿里云计算有限公司	1	1
南京众智维信息科技有限公司	145	145
北京山石网科信息技术有限公司	132	132
国瑞数码零点实验室	108	108
新疆海狼科技有限公司	107	107
上海犀点意象网络科技有限公司	94	94
河南信安世纪科技有限公司	84	84
山东新潮信息技术有限公司	63	63
北京天地和兴科技有限公司	48	48
江苏保旺达软件技术有限公司	38	38
远江盛邦（北京）网络安全科技股份有限公司	36	36
山东华鲁科技发展股份有限公司	34	34
河南灵创电子科技有限公司	26	26
西安交大捷普网络科技有限公司	22	22
安徽长泰信息安全服务有限公司	19	19
任子行网络技术股份有限公司	13	13
内蒙古奥创科技有限公司	12	12
山东云天安全技术有限公司	10	10
北京中科微澜科技有限公司	9	9

重庆贝特计算机系统工程有限公司	9	9
北京华顺信安科技有限公司	8	0
北京顶象技术有限公司	8	8
北京信联科汇科技有限公司	8	8
吉林谛听信息技术有限公司	7	7
京东云安全	5	5
木链科技	5	5
上海市信息安全测评认证中心	5	5
北京机沃科技有限公司	4	4
广州市蓝爵计算机科技有限公司	4	4
四川哨兵信息科技有限公司	4	4
北京惠而特科技有限公司	3	3
北京圣博润高新技术股份有限公司	3	3
北京长亭科技有限公司	3	3
上海观安信息技术股份有限公司	3	3
武汉明嘉信信息安全检测评估有限公司	3	3
北京明朝万达科技股份有限公司	2	2
湖南浩基信息技术有限公司	2	2
北京时代新威信息技术有限公司	1	1
北京智游网安科技有限公司	1	1
平安银河实验室	1	1
上海崤函信息科技有限公司	1	1
重庆都会信息科技	1	1
CNCERT 宁夏分中心	24	24
CNCERT 山西分中心	12	12
CNCERT 浙江分中心	7	7
CNCERT 山东分中心	3	3
CNCERT 西藏分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 青海分中心	1	1
个人	757	757
报送总计	7337	6101

本周漏洞按类型和厂商统计

本周，CNVD 收录了 378 个漏洞。应用程序 194 个，WEB 应用 63 个，网络设备（交换机、路由器等网络端设备）42 个，操作系统 28 个，安全产品 5 个，智能设备（物联网终端设备）3 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	194
WEB 应用	63
网络设备（交换机、路由器等网络端设备）	42
操作系统	28
安全产品	5
智能设备（物联网终端设备）	3

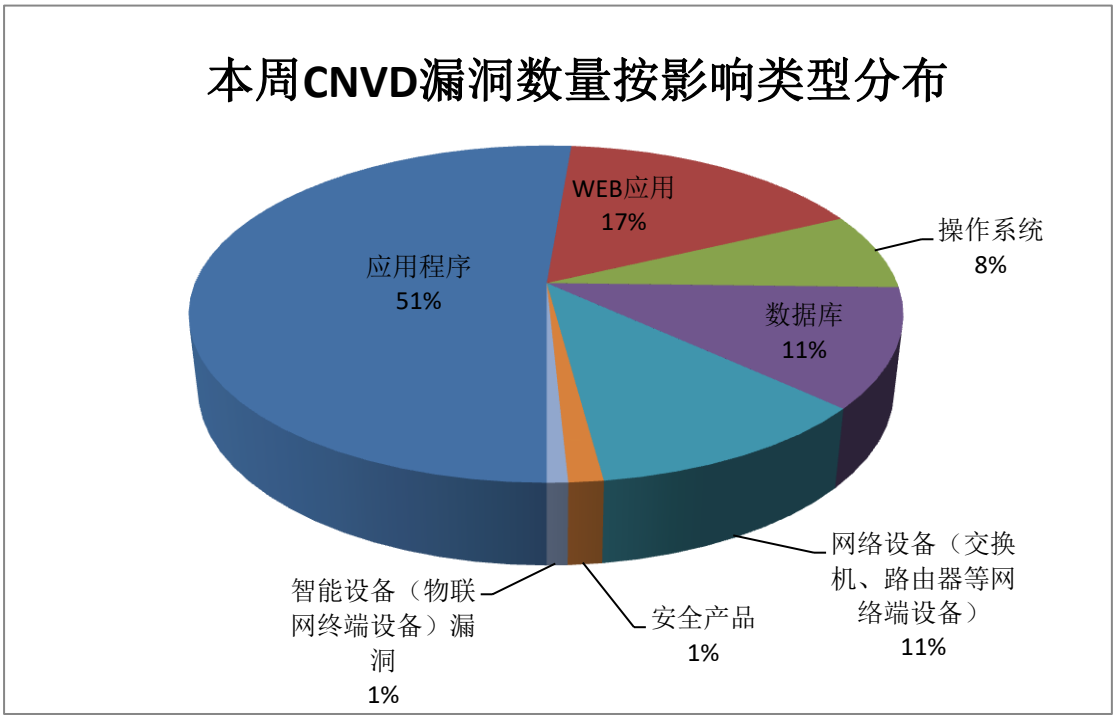

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Mozilla、Cisco 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	Oracle	45	12%
2	Mozilla	34	9%
3	Cisco	25	7%
4	Google	25	7%
5	WordPress	18	5%

6	SAP	15	4%
7	Foxit	12	3%
8	北京海腾时代科技有限公司	10	3%
9	AdRem	8	2%
10	其他	186	48%

本周行业漏洞收录情况

本周，CNVD 收录了 43 个电信行业漏洞，9 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Marvell QConvergeConsole GUI 路径遍历漏洞、DOPSoft 空指针解引用漏洞、DOPSoft 越界写入漏洞”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/

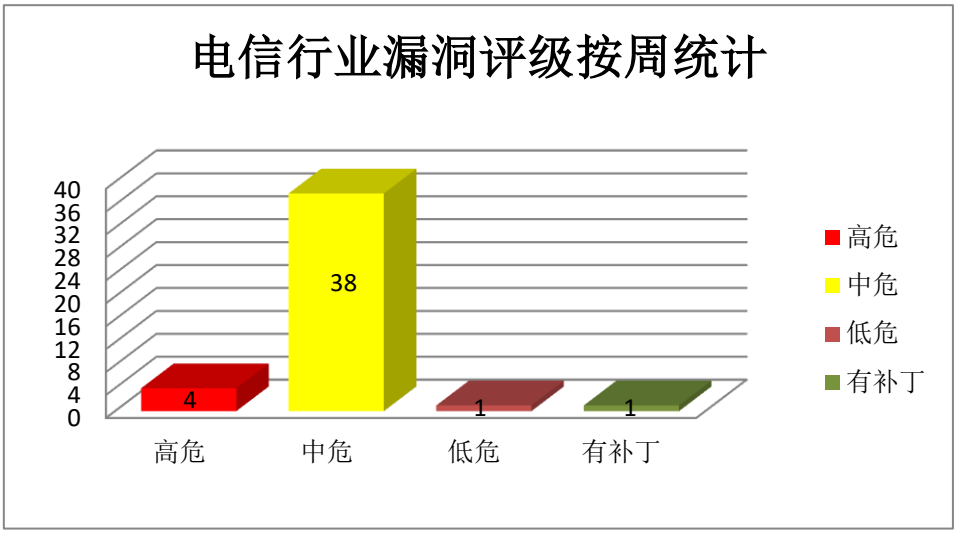

图 3 电信行业漏洞统计

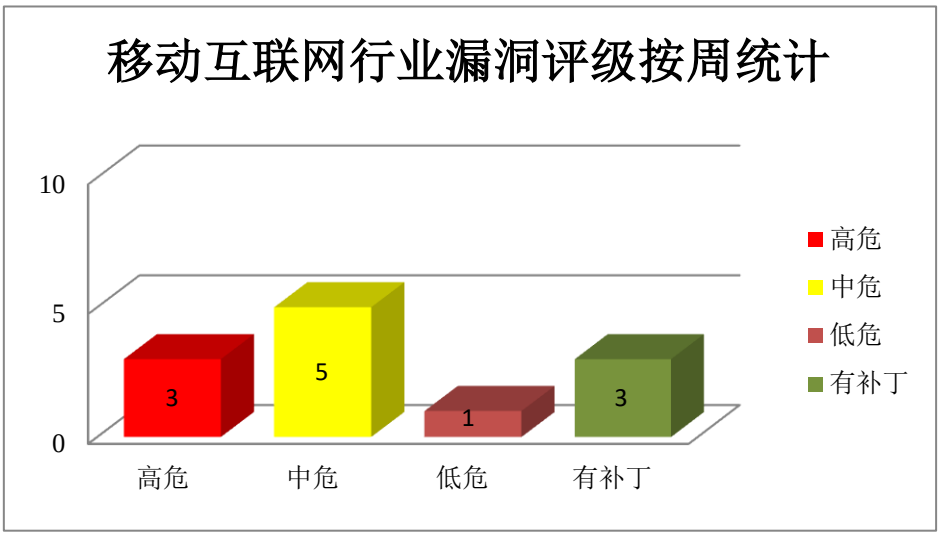

图 4 移动互联网行业漏洞统计

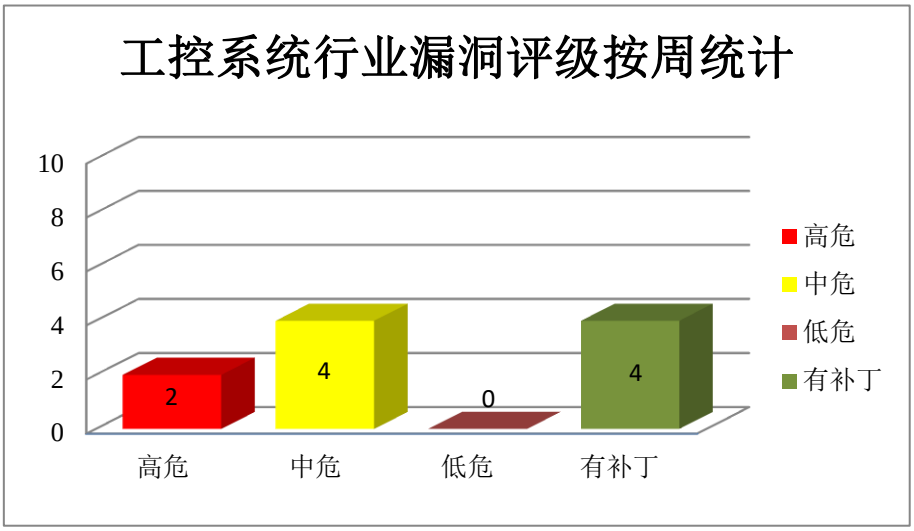

图 5 工控系统行业漏洞统计

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、SAP 产品安全漏洞

SAP NetWeaver Master Data Management（SAP MDM）是德国 SAP 公司的一款用于管理企业间协同合作的软件。SAP Netweaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台。该平台主要为 SAP 应用程序提供开发和运行环境。SAP Banking Services 是德国思爱普（SAP）公司的一套银行服务解决方案。SAP BusinessObjects Business Intelligence Platform 是德国思爱普（SAP）公司的一套商业智能软件和企业绩效解决方案套件。该产品具有报告生成、分析和数据可视化等功能。SAP NetWeaver AS ABAP Business Server 是德国思爱普（SAP）公司的一款适用于 ABAP（高级商务应用编程）的应用服务器。SAP S/4 HANA 和 SAP ERP 都是德国思爱普（SAP）

公司的产品。SAP S/4 HANA 是一款适用于大型企业的智能化集成式 ERP 软件。SAP ERP 是一系列用于 ERP 管理的软件。SAP NetWeaver Application Server 是德国思爱普（SAP）公司的一款应用程序服务器。SAP HCM Travel Management 是德国思爱普（SAP）公司的一个差旅管理模块。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，进行权限提升，使应用崩溃等。

CNVD 收录的相关漏洞包括：SAP NetWeaver Master Data Management 信息泄露漏洞（CNVD-2021-03698）、SAP Netweaver AS ABAP 资源管理错误漏洞、SAP Banking Services 权限提升漏洞、SAP Netweaver AS JAVA 授权问题漏洞、SAP BusinessObjects Business Intelligence Platform XML 外部实体注入漏洞、SAP NetWeaver AS ABAP 跨站脚本漏洞（CNVD-2021-03703）、SAP ERP 和 SAP S/4 HANA 授权问题漏洞（CNVD-2021-03707）、SAP NetWeaver Application Server Java 跨站脚本漏洞。其中，“SAP Netweaver AS JAVA 授权问题漏洞”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-2021-03698
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03701
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03699
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03705
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03704
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03703
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03707
https://www.cnvd.org.cn/flaw/show/CNVD-2021-03711

2、Foxit 产品安全漏洞

Foxit Reader 和 Foxit PhantomPDF 都是中国福昕（Foxit）公司的一款 PDF 文档阅读器。Foxit PDF SDK ActiveX 是中国福昕（Foxit）公司的一个 PDF 软件开发工具包，也是一个可视化编程组件。该产品提供 PDF 显示及注释等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致堆栈缓冲区溢出或越界读取，远程执行代码等。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 竞争条件漏洞（CNVD-2021-04397、CNVD-2021-04399、CNVD-2021-04398、CNVD-2021-04401、CNVD-2021-04400、CNVD-2021-04403、CNVD-2021-04402）、Foxit PDF SDK ActiveX 命令注入漏洞。其中，“Foxit PDF SDK ActiveX 命令注入漏洞”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-2021-04397
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04396

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04399

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04398

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04401

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04400

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04403

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04402

3、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在两个蓝牙设备之间远程升级特权，而无需其他执行特权，导致本地特权提升，获取服务器控制权限。

CNVD 收录的相关漏洞包括：Google Android System 远程代码执行漏洞（CNVD-2021-04374）、Google Android System 权限提升漏洞（CNVD-2021-04373、CNVD-2021-04372）、Google Android Media Framework 信息泄露漏洞（CNVD-2021-04376、CNVD-2021-04375）、Google Android Framework 信息泄露漏洞（CNVD-2021-04379）、Google Chrome 资源管理错误漏洞（CNVD-2021-04393）、Google Chrome 内存错误引用漏洞（CNVD-2021-04421）。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-2021-04374

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04373

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04372

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04376

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04375

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04379

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04393

https://www.cnvd.org.cn/flaw/show/CNVD-2021-04421

4、Mozilla 产品安全漏洞

Mozilla Firefox 和 Mozilla Firefox ESR 都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是由 Mozilla 浏览器的邮件功能部件所改造的邮件工具，使用 XUL 程序界面语言所设计，是专门为搭配 Mozilla Firefox 浏览器使用者所设计的邮件客户端软件，界面设计更简洁、而且免安装。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞控制标签的内容，同时 URL 栏显示原始域，交特殊的 WEB 请求，诱使用户解析，可使应用程序崩溃或可以应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 输入验证错误漏洞（CNVD-2021-04654）、Mozilla Firefox 资源管理错误漏洞（CNVD-2021-04744）、Mozilla Firefox 跨站脚本漏洞（CNVD-2021-04748）、Mozilla Firefox 内存破坏漏洞（CNVD-2021-04747）、Mozilla Firefox ESR 缓冲区溢出漏洞（CNVD-2021-04746）、Mozilla Firefox ESR 跨站脚本漏洞（CNVD-2021-04745）、Mozilla Thunderbird/Firefox ESR 释放后重用漏洞、Mozilla Firefox 代码执行漏洞（CNVD-2021-04749）。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-2021-04654
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04744
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04748
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04747
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04746
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04745
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04750
https://www.cnvd.org.cn/flaw/show/CNVD-2021-04749

5、TP-Link TL-WR840N OS 命令注入漏洞

TP-LINK TL-WR840N 是一款无线路由器，信道数为 13，支持 VPN 功能。本周，TP-Link TL-WR840N 被披露存在 OS 命令注入漏洞。攻击者可利用该漏洞注入 OS 命令。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-2021-04412

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-2021-03993	Linux kernel 任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5c455c5ab332773464d02ba17015acdca198f03d
CNVD-2021-04358	WordPress Quiz and Survey Master plugin 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.wordfence.com/blog/2020/08/critical-vulnerabilities-patched-in-quiz-and-survey-master-plugin/
CNVD-2021-	wolfSSL 越界写入漏洞	高	厂商已发布相关漏洞补丁链接，请及

04411			时更新：https://github.com/wolfSSL/wolfssl/releases/tag/v4.6.0-stable
CNVD-2021-04428	Crimson 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://www.redlion.net/support/software-firmware/red-lion-software/crimson/crimson-31
CNVD-2021-04430	DOPSoft 越界写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&CID=06&itemID=060302&dataType=8&q=DOPSoft
CNVD-2021-04784	Rust 资源管理错误漏洞（CNVD-2021-04784）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/rusqlite/rusqlite/releases/tag/0.23.0
CNVD-2021-04819	FortiWeb 栈缓冲区溢出漏洞	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-20-125
CNVD-2021-04821	Element OS 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，详情请关注厂商主页：https://security.netapp.com/advisory/ntap-20210108-0008/
CNVD-2021-05110	Oracle Weblogic 远程代码执行漏洞	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/cpujan2021.html
CNVD-2021-05125	DELL EMC Avamar Server 路径遍历漏洞（CNVD-2021-05125）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000181806/dsa-2020-272-dell-emc-avamar-server-security-update-for-multiple-vulnerabilities

小结：本周，SAP 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，进行权限提升，使应用崩溃等。此外，Foxit、Google、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致堆栈缓冲区溢出或越界读取，远程执行代码，获取服务器控制权限等。另外，TP-Link TL-WR840N 被披露存在 OS 命令注入漏洞。攻击者可利用该漏洞注入 OS 命令。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、JIZHICMS 跨站脚本漏洞

验证描述

JIZHICMS（极致 CMS）是一款开源免费、无商业授权的建站系统。

JIZHICMS 1.7.1 中的 Home/c/ErrorController.php 存在跨站脚本漏洞。攻击者可通过 index.php/Error/index?msg={XSS]利用该漏洞注入任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/Cherry-toto/jizhicms/issues/28

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-04409

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. 多个 Linux 发行版考虑移除 Chromium 软件包

Google Chrome Team 团队向 Linux 发行版开发者发去邮件通知，从 3 月 15 日起，在构建配置中使用 google_default_client_id 和 google_default_client_secret 的第三方 Chromium 版本，它们的终端用户将无法再登陆其 Google Accounts 账号。

参考链接：https://www.solidot.org/story?sid=66710

2. CISCO 修复了 SD-WAN，云许可证管理器中的关键预身份验证错误

思科已发布安全更新，以解决影响多个 SD-WAN 产品和 Cisco Smart Software Manager 软件的预认证远程代码执行（RCE）漏洞。SD-WAN 是有助于管理广域网（WAN）的软件产品，而 Smart Software Manager 是用于 Cisco 许可证的基于云的管理解决方案。

参考链接：https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-pre-auth-bugs-in-sd-wan-cloud-license-manager/

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