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 24 日-2021 年 05 月 30 日　　2021 年第 21 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 604 个，其中高危漏洞 143 个、中危漏洞 379 个、低危漏洞 82 个。漏洞平均分值为 5.52。本周收录的漏洞中，涉及 0day 漏洞 223 个（占 37%），其中互联网上出现“Multilaser Router AC1200 跨站请求伪造漏洞、MyLittleAdmin 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 2984 个，与上周（3079 个）环比减少 3%。

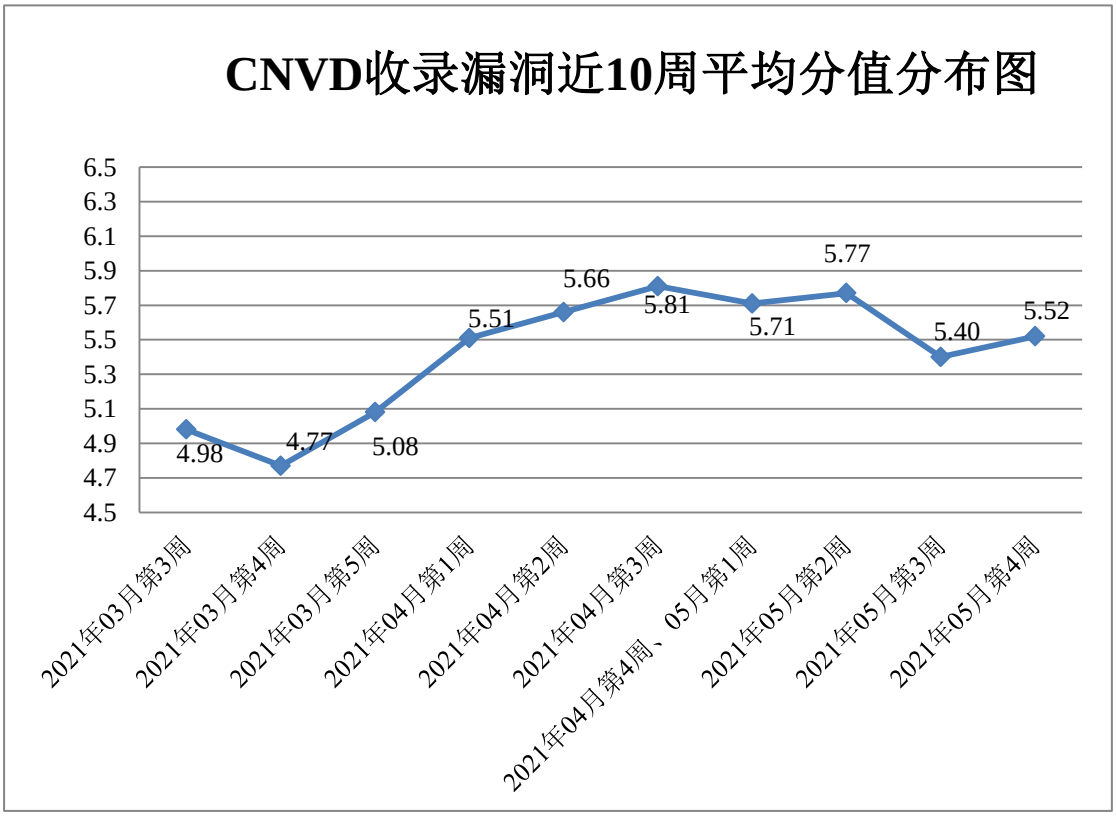

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 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 490 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 43 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：

淄博闪灵网络科技有限公司、郑州微厦计算机科技有限公司、正方软件股份有限公司、运城市盘石网络科技有限公司、友讯电子设备（上海）有限公司、优酷信息技术（北京）有限公司、用友网络科技股份有限公司、西门子（中国）有限公司、武汉中地数码科技有限公司、武汉玖玖珈网络科技有限公司、无锡信捷电气股份有限公司、维沃移动通信（深圳）有限公司、唯智信息技术（上海）股份有限公司、微宏软件技术（杭州）有限公司、天信仪表集团有限公司、天津黑核科技有限公司、泰安梦泰尔软件有限公司、四平市九州易通科技有限公司、四创科技有限公司、四川易泊时捷智能科技有限公司、四川迅游网络科技股份有限公司、四川五佳网络科技有限公司、四川方法数码科技有限公司、石家庄和嘉科技有限公司、深圳维盟科技股份有限公司、深圳搜豹网络有限公司、深圳市中科网威科技有限公司、深圳市英威腾电气股份有限公司、深圳市鑫星空软件有限公司、深圳市微耕实业有限公司、深圳市网域科技技术有限公司、深圳市万网博通投资管理有限合伙企业、深圳市硕赢互动信息技术有限公司、深圳市明源云科技有限公司、深圳市利谱信息技术有限公司、深圳市惠尔顿信息技术有限公司、深圳市大世同舟信息科技有限公司、深圳市百为通达科技有限公司、深圳警翼智能科技股份有限公司、上海迅饶自动化科技有限公司、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、上海顶想信息科技有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山东科德电子有限公司、山东康网网络技术有限公司、山东聚恒网络技术有限公司、厦门市灵鹿谷科技有限公司、三盟科技股份有限公司、睿易教育科技股份有限公司、任子行网络技术股份有限公司、普联技术有限公司、宁波互明科技有限公司、雷神科技有限公司、浪潮集团有限公司、廊坊市极致网络科技有限公司、江苏易索电子科技股份有限公司、江苏三希科技股份有限公司、淮南市讯网信息技术有限公司、华硕电脑（上海）有限公司、湖南聚匠科技有限公司、湖南翱云网络科技有限公司、洪湖尔创网联信息技术有限公司、河南青否网络科技有限公司、杭州海康威视系统技术有限公司、杭州海康威视数字技术股份有限公司、汉王科技股份有限公司、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、广州安网通信技术有限公司、广西唐宋软件有限公司、广西日报传媒集团有限公司、福建智度科技有限公司、福建博思软件股份有限公司、佛

山云迈电子商务有限公司、帆软软件有限公司、东华软件股份公司、盯盯拍（深圳）技术股份有限公司、成都星锐蓝海网络科技有限公司、成都新线加科技有限公司、成都市智蜂网科技有限责任公司、成都德芯数字科技股份有限公司、北京卓导科技有限公司、北京中科网威信息技术有限公司、北京中创视讯科技有限公司、北京原创先锋网络科技发展有限公司、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、北京网康科技有限公司、北京搜狐互联网信息服务有限公司、北京硕人时代科技股份有限公司、北京世纪长秋科技有限公司、北京齐鲁泓霖科技有限公司、北京领英信息技术有限公司、北京猎豹网络科技有限公司、北京朗新天霁软件技术有限公司、北京火绒网络科技有限公司、北京火木科技有限公司、北京宏景世纪软件有限公司、北京和利时集团、北京百卓网络技术有限公司、北京奥泰瑞格科技有限公司、安美世纪（北京）科技有限公司、上海荃路软件开发工作室、联想全球安全实验室、帝国软件、百度安全应急响应中心、狂雨小说 cms、鱼跃 CMS、若依、zzzcms、zzcms、yycms、YFCMF、xhcms2、XHCMS、semcms、KiteCMS、Joomla、Google、EacooPHP、Dreamer CMS、BEESCMS、Axis Communications、Belkin International,Inc 和 Adobe。

本周，CNVD 发布了《关于 VMware vCenter Server 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/6461

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、北京数字观星科技有限公司、深信服科技股份有限公司、华为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、北京信联科汇科技有限公司、新疆海狼科技有限公司、安徽长泰信息安全服务有限公司、河南信安世纪科技有限公司、江西省掌控者信息安全技术有限公司、北京山石网科信息技术有限公司、河南灵创电子科技有限公司 、北京安帝科技有限公司、北京天地和兴科技有限公司、山东云天安全技术有限公司、上海纽盾科技股份有限公司、杭州木链物联网科技有限公司、四川哨兵信息科技有限公司、福建省海峡信息技术有限公司、联想全球安全实验室、广州安亿信软件科技有限公司、浙江大学控制科学与工程学院、上海市信息安全测评认证中心、武汉绿色网络信息服务有限责任公司、武汉明嘉信信息安全检测评估有限公司、新疆天山智汇信息科技有限公司、浙江东安检测技术有限公司、浙江御安信息技术有限公司、中移（杭州）信息技术有限公司、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 2984 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 1867 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）	839	839
奇安信网神（补天平台）	555	555
上海交大	473	473
北京神州绿盟科技有限公司	255	6
新华三技术有限公司	154	0
北京数字观星科技有限公司	108	0
深信服科技股份有限公司	100	0
华为技术有限公司	91	0
哈尔滨安天科技集团股份有限公司	89	0
恒安嘉新（北京）科技股份公司	62	0
国瑞数码零点实验室	50	0
卫士通信息产业股份有限公司	31	0
西安四叶草信息技术有限公司	26	26
北京奇虎科技有限公司	7	7
北京天融信网络安全技术有限公司	7	5
杭州安恒信息技术股份有限公司	6	6
北京知道创宇信息技术股份有限公司	3	1
远江盛邦（北京）网络安全科技股份有限公司	3	3
南京联成科技发展股份有限公司	1	1
北京华顺信安科技有限公司	169	0
南京众智维信息科技有限公司	59	59
北京信联科汇科技有限公司	58	58
新疆海狼科技有限公司	49	49

安徽长泰信息安全服务有限公司	28	28
河南信安世纪科技有限公司	27	27
江西省掌控者信息安全技术有限公司	23	23
中国电信股份有限公司网络安全产品运营中心	20	0
北京山石网科信息技术有限公司	17	17
杭州迪普科技股份有限公司	15	0
河南灵创电子科技有限公司	14	14
北京安帝科技有限公司	11	11
北京天地和兴科技有限公司	11	11
山东云天安全技术有限公司	11	11
上海纽盾科技股份有限公司	9	9
杭州木链物联网科技有限公司	8	8
四川哨兵信息科技有限公司	5	5
西门子（中国）有限公司	5	0
福建省海峡信息技术有限公司	3	3
联想全球安全实验室	3	3
广州安亿信软件科技有限公司	2	2
浙江大学控制科学与工程学院	2	2
上海市信息安全测评认证中心	1	1
武汉绿色网络信息服务有限责任公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
新疆天山智汇信息科	1	1

技有限公司		
浙江东安检测技术有限公司	1	1
浙江御安信息技术有限公司	1	1
中移（杭州）信息技术有限公司	1	1
北京机沃科技有限公司	1	1
CNCERT 天津分中心	15	15
CNCERT 宁夏分中心	12	12
CNCERT 贵州分中心	9	9
CNCERT 山西分中心	8	8
CNCERT 青海分中心	6	6
CNCERT 浙江分中心	5	5
CNCERT 河北分中心	3	3
CNCERT 海南分中心	2	2
个人	654	654
报送总计	4131	2984

本周漏洞按类型和厂商统计

本周，CNVD 收录了 604 个漏洞。应用程序 329 个，WEB 应用 165 个，网络设备（交换机、路由器等网络端设备）65 个，操作系统 18 个，智能设备（物联网终端设备）17 个，安全产品 9 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	329
WEB 应用	165
网络设备（交换机、路由器等网络端设备）	65
操作系统	18
智能设备（物联网终端设备）	17
安全产品	9
数据库	1

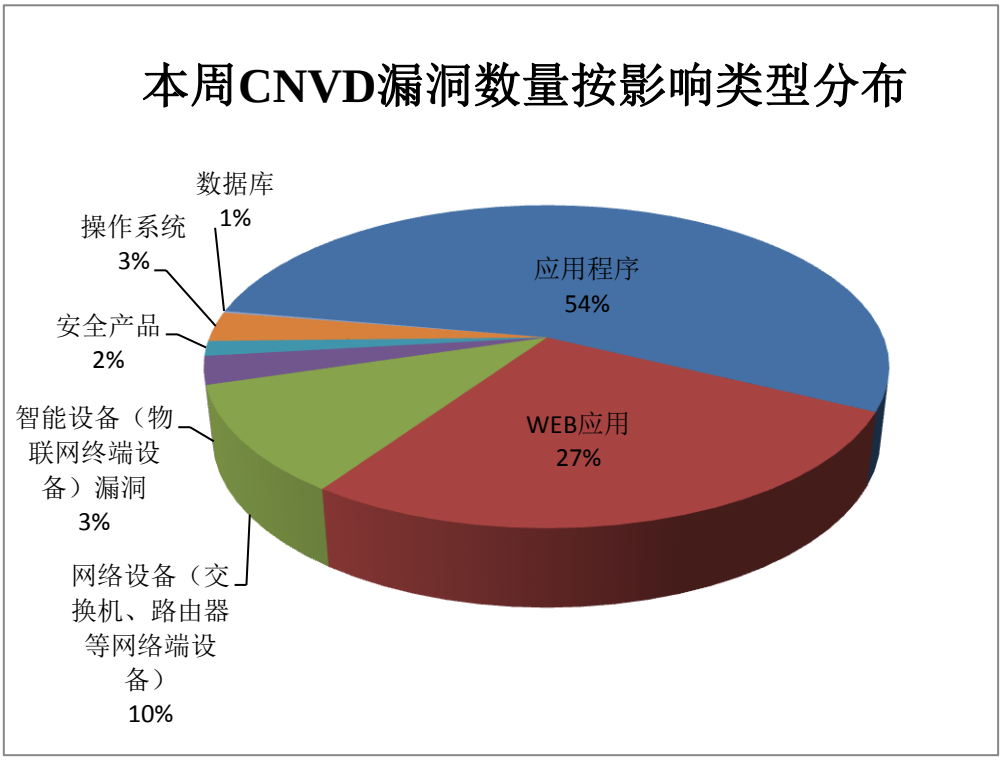

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、Oracle 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	Google	57	9%
2	Cisco	30	5%
3	Oracle	27	5%
4	IBM	25	4%
5	GNU	24	4%
6	NETGEAR	17	3%
7	WordPress	13	2%
8	Libwebp	12	2%
9	Nagios	12	2%
10	其他	387	64%

本周行业漏洞收录情况

本周，CNVD 收录了 48 个电信行业漏洞，6 个移动互联网行业漏洞，23 个工控行业漏洞（如下图所示）。其中，“Cisco SD-WAN vEdge 缓冲区溢出漏洞、Samsung Galaxy S5 缓冲区溢出漏洞、3S-Smart Software Solutions CODESYS V2 Web-Server 越界写入漏洞、Siemens SmartVNC 内存越界访问漏洞”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/

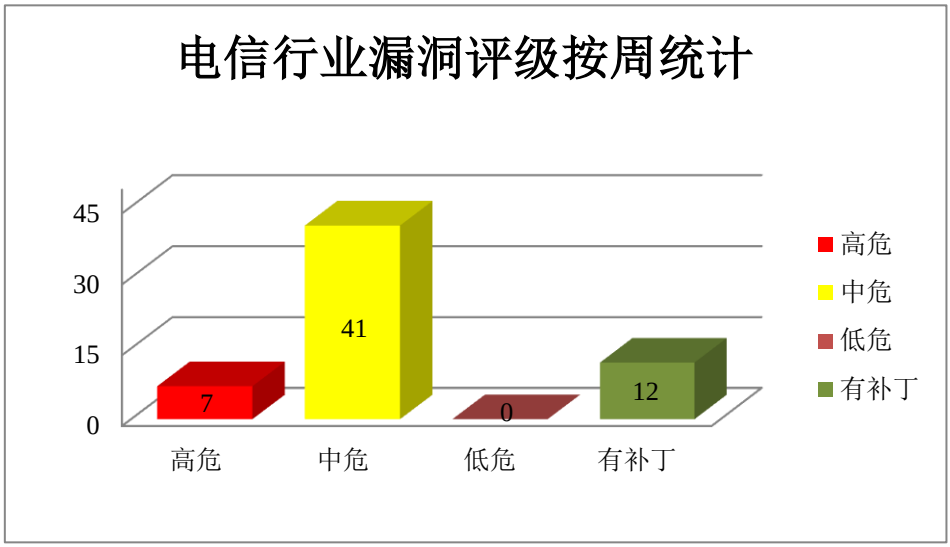

图 3 电信行业漏洞统计

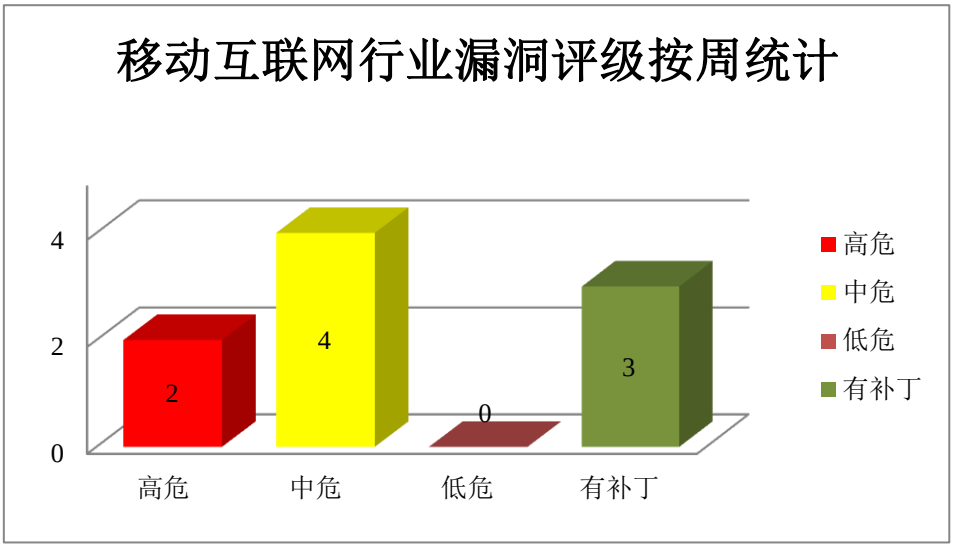

图 4 移动互联网行业漏洞统计

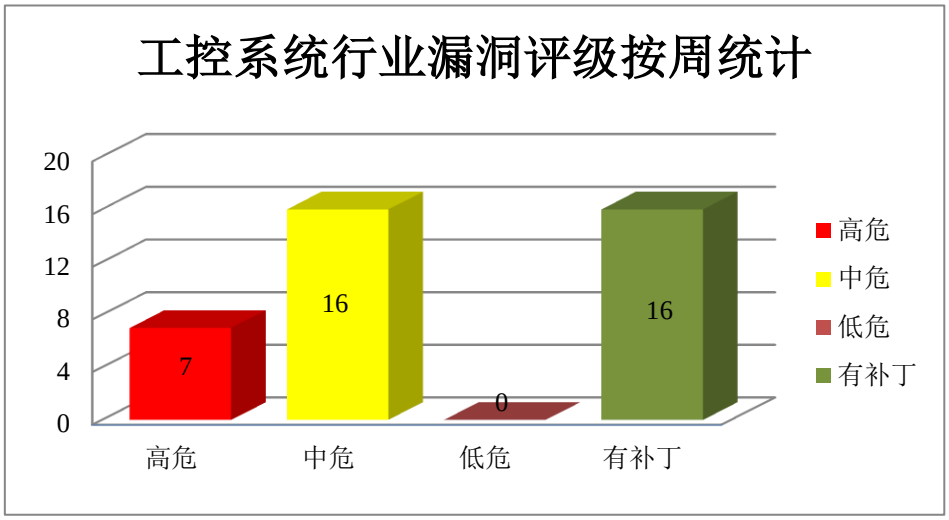

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Audio driver 是其中的一个音频驱动程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务，导致“Conv2DBackpropFilter”中发生堆缓冲区溢出等。

CNVD 收录的相关漏洞包括：Google TensorFlow RaggedBinCount 拒绝服务漏洞（CNVD-2021-37606、CNVD-2021-37607）、Google TensorFlow 拒绝服务漏洞（CNVD-2021-37609、CNVD-2021-37632）、Google TensorFlow QuantizedReshape 拒绝服务漏洞、Google TensorFlow Conv2DBackpropFilter 拒绝服务漏洞、Google TensorFlow Quantized ResizeBilinear 拒绝服务漏洞、Google TensorFlow SparseDenseCwiseMul 堆越界访问漏洞。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-2021-37606

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37609

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37607

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37614

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37618

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37615

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37632

https://www.cnvd.org.cn/flaw/show/CNVD-2021-37640

2、Cisco 产品安全漏洞

Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。Cisco DNA Spaces 是美国思科（Cisco）公司的一套室内定位服务平台。Cisco SD-WAN vEdge 是美国思科（Cisco）公司的是一款路由器。该设备可为思科 SD-WAN 解决方案提供基本 WAN，安全性和多云功能。Cisco Enterprise NFV Infrastructure Software 是一款轻量级虚拟化平台，将完整的 VM 生命周期管理、监控、设备可编程性及服务链集成在了一个可安装的软件包中。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 特权在底层操作系统上执行任意代码，导致缓冲区溢出，发送大量 API 请求导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Finesse 跨站脚本漏洞（CNVD-2021-36553）、Cisco SD-WAN vManage Software 缓冲区溢出漏洞、Cisco DNA Spaces 操作系统命令注入漏洞、Cisco DNA Spaces Connector 操作系统命令注入漏洞、Cisco SD-WAN vManage 拒绝服务漏洞、Cisco SD-WAN vEdge 缓冲区溢出漏洞、Cisco Enterprise NFV Infrastructure Software 命令注入漏洞、Cisco SD-WAN vManage 授权问题漏洞。其中，除“Cisco Finesse 跨站脚本漏洞（CNVD-2021-36553）”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-2021-36553
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37062
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37123
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37476
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37684
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37682
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37688
https://www.cnvd.org.cn/flaw/show/CNVD-2021-37687

3、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。LTS 是 CloudBeesJenkins 的一个长期支持版本。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指定的凭据 ID 连接至指定的 URL，从而获取存储在 Jenkins 中的凭据，通过使用指定的用户名和密码连接至其指定的 Perforce 服务器，获取已配置的配置文件的列表，发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins Xray - Test Management for Jira Plugin 跨站请求伪造漏洞、CloudBees Jenkins Xray - Test Management for Jira Plugi

n 授权问题漏洞、CloudBees Jenkins P4 Plugin 跨站请求伪造漏洞、CloudBees Jenkins P4 Plugin 访问控制错误漏洞、CloudBees Jenkins S3 publisher Plugin 授权问题漏洞（CNVD-C-2021-118103）、CloudBees Jenkins Xcode integration Plugin XML 外部实体注入漏洞、CloudBees Jenkins CloudBees CD Plugin 授权问题漏洞、CloudBees Jenkins Credentials Plugin 跨站脚本漏洞。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-2021-36577

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36576

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36582

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36581

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36579

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36578

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36585

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36584

4、SAP 产品安全漏洞

SAP Process Integration 是德国 SAP 公司提供的一种中间件，可使 SAP 与公司中的非 SAP 应用程序或公司外部的系统进行无缝集成。SAP GUI 是德国思爱普（SAP）公司的一个应用软件。SAP 系统的图形用户界面。SAP Commerce 是德国思爱普（SAP）公司的一套基于云的电子商务平台。该产品支持销售管理、营销管理、订单管理和运营管理等。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 NetWeaver Application Server（AS）Java 是一款运行于 NetWeaver 中且基于 Java 编程语言的应用服务器。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 Solution Manager 是德国思爱普（SAP）公司的一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。该平台可以帮助客户建立 SAP 解决方案的生命周期管理，并提供系统监控、远程支持服务和 SAP 产品组件升级等功能。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拒绝服务，可以创建恶意 XML，当应用程序上载和解析该 XML 时，可能会由于消耗大量系统内存而导致拒绝服务情况，从而严重影响系统可用性，窃取受害者的凭据，执行 ABAP 报告注入恶意代码利用该漏洞访问数据、覆盖数据或导致拒绝服务等。

CNVD 收录的相关漏洞包括：SAP Process Integration 权限许可和访问控制问题漏洞（CNVD-2021-36675、CNVD-2021-36676）、SAP GUI 输入验证错误漏洞、SAP Commerce 信息泄露漏洞（CNVD-2021-36678）、SAP NetWeaver AS ABAP 代码注入漏洞、SAP NetWeaver Application Server for Java 访问控制错误漏洞、SAP NetWeaver Master Data Management 信息泄露漏洞（CNVD-2021-36683）、SAP Solution Manager 信息

泄露漏洞。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-2021-36676

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36675

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36674

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36678

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36677

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36684

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36683

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36682

5、IBM Security Guardium 命令执行漏洞

IBM Security Guardium 是美国 IBM 公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。本周，IBM Security Guardium 被披露存在命令执行漏洞。攻击者可利用该漏洞通过发送专门设计的请求在系统上执行任意命令。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-2021-37119

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-2021-36557	MikroTik RouterOS 除零错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://mikrotik.com/
CNVD-2021-36599	VMware vRealize Business for Cloud 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.vmware.com/security/advisories/VMSA-2021-0007.html
CNVD-2021-36607	Drupal 跨站请求伪造漏洞（CNVD-2021-36607）	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.drupal.org/sa-core-2020-004
CNVD-2021-36665	Proofpoint Insider Threat Management Server 远程代码执行漏洞（CNVD-2021-36665）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.proofpoint.com/us/security/security-advisories/pfpt-sa-2020-0003
CNVD-2021-36670	LAOBANCMS 任意文件上传漏洞	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/Cumtyuanfeng/Laobancms/blob/master/vuln.md
CNVD-2021-36681	GNU Binutils 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugzilla.redhat.com/show_bug.cgi?id=1947111
CNVD-2021-36844	CentOS Web Panel 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：http://centos-webpanel.com/
CNVD-2021-36848	Synology Surveillance Station 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.qnap.com/en/security-advisory/qsa-21-07
CNVD-2021-36850	Eclipse Mosquitto 访问控制错误漏洞	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.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-2021-tibco-messaging-2021-28826
CNVD-2021-37052	HPE iLO Amplifier Pack 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://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04129en_us

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务，导致“Conv2DBackpropFilter”中发生堆缓冲区溢出等。此外，Cisco、CloudBees、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞以 root 特权在底层操作系统上执行任意代码，导致缓冲区溢出，通过指定的凭据 ID 连接至指定的 URL，从而获取存储在 Jenkins 中的凭据，通过使用指定的用户名和密码连接至其指定的 Perforce 服务器，获取已配置的配置文件的列表，发起跨站脚本攻击等。另外，IBM Security Guardium 被披露存在命令执行漏洞。攻击者可利用漏洞通过发送专门设计的请求在系统上执行任意命令。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、Multilaser Router AC1200 跨站请求伪造漏洞

验证描述

Multilaser Router AC1200 是 Multilaser 公司的一个路由器。

Multilaser Router AC1200 V02.03.01.45_pt 存在跨站请求伪造漏洞，攻击者可利用该漏洞通过配置错误的请求、条目和报头启用远程访问、更改密码和执行其他操作。

验证信息

POC 链接：https://packetstormsecurity.com/files/162258/Multilaser-Router-RE018-AC1200-Cross-Site-Request-Forgery.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-36851

信息提供者

恒安嘉新（北京）科技股份公司

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. 一个关键漏洞影响所有 VMware vCenter Server 的安装

VMware 解决了 Virtual SAN Health Check 插件中的一个关键的远程代码执行（RCE）漏洞，该漏洞影响了所有 vCenter Server 安装。

参考链接：https://securityaffairs.co/wordpress/118271/security/vmware-vcenter-server-cve-2021-21985.html

2. 研究人员发现在签名过程中篡改已认证 PDF 的技术

德国的研究人员发现有人可以用数字方式将自己的签名添加到 PDF 文件中，例如将一份合同传递给另一个伙伴进行数字签名，而第二个人可以偷偷地改变合同的文本并进行签名，从而造成混乱。

参考链接：https://www.theregister.com/2021/05/26/pdf_certificate_flaw/?&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