国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 06 月 15 日-2020 年 06 月 21 日　　2020 年第 25 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 483 个，其中高危漏洞 126 个、中危漏洞 294 个、低危漏洞 63 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 39%），其中互联网上出现“Submitty 跨站脚本漏洞、Cellebrite UFED 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 3718 个，与上周（2100 个）环比增加 77%。

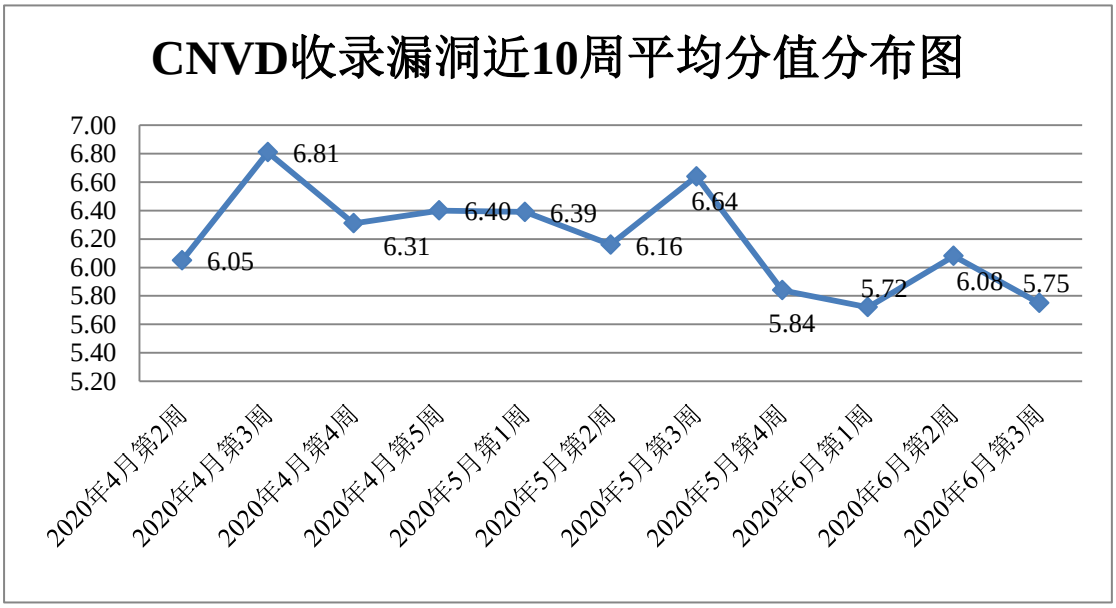

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 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 284 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 39 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 24 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：

开平市联科网络科技有限公司、佛山市顺的网络工程有限公司、上海秀派电子科技股份有限公司、杭州临企网络技术有限公司、酷溜网（北京）文化传媒有限公司、镇江市云优网络科技有限公司、北京良精志诚科技有限责任公司、珠海金山办公软件有限公司、宿迁鑫潮信息技术有限公司、深圳市显控科技股份有限公司、上海卓卓网络科技有限公司、北京天盈九州网络技术有限公司、茉柏枘（上海）软件科技有限公司、杭州达勒网络信息技术有限公司、正知（上海）智能技术有限公司、数字天堂(北京)网络技术有限公司、上海亿速网络科技有限公司、江苏物润船联网络股份有限公司、成都无标度网络科技有限公司、用友网络科技股份有限公司、赤峰易拓网络有限公司、合肥蓝领商务信息有限公司、研华科技（中国）有限公司、哈尔滨伟成科技有限公司、校无忧科技网络公司、北京央融科技发展集团有限公司、长沙米拓信息技术有限公司、成都康菲顿特网络科技有限公司、华语数媒（北京）科技有限公司、成都康菲顿特网络科技有限公司、华语数媒（北京）科技有限公司、深圳警翼智能科技股份有限公司、深圳市果谷网络有限公司、东莞市智跃软件科技有限公司、临沂新报网络科技有限公司、苏州乐艺网络科技有限公司、济南卓源软件有限公司、重庆猫扑网络科技有限公司、上海欧虎网络科技有限公司、浙江宇视科技有限公司、许昌永诚网络科技有限公司、宁波斯博网络科技有限公司、深圳锟锷科技有限公司、广州市三今网络技术有限公司、广东世纪信通网络科技有限公司、联想（北京）有限公司、易族智汇（北京）科技有限公司、广东布恩网络有限公司、济南速动信息科技有限公司、济南亘安信息技术有限公司、四川迅睿云软件开发有限公司、点拓科技、北京市海淀区融媒体中心、DM 企业建站系统、发货 100、贴心猫(imcat)、ZZCMS、Guojiz、DuomiCms、OSGeo、MM-Wiki、KUKA、Adobe、VMware, Inc.、VIRTUAL AIRLINES MANAGER 和 Zabbix。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，恒安嘉新(北京)科技股份公司、哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、北京华云安信息技术有限公司、河南灵创电子科技有限公司、吉林谛听信息技术有限公司、山东云天安全技术有限公司、济南三泽信息安全测评有限公司、广州竞远安全技术股份有限公司、南京众智维信息科技有限公司、山东道普测评技术有限公司、河北华测信息技术有限公司、内蒙古奥创科技有限公司、上海观安信息技术股份有限公

司、北京智游网安科技有限公司、安徽长泰信息安全服务有限公司、上海纽盾科技股份有限公司、京东云安全、北京浩瀚深度信息技术股份有限公司、北京顶象技术有限公司、北京神荼科技有限公司及其他个人白帽子向 CNVD 提交了 3718 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 3029 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
奇安信网神（补天平台）	1785	1785
斗象科技（漏洞盒子）	799	799
上海交大	445	445
恒安嘉新(北京)科技股份公司	285	0
哈尔滨安天科技集团股份有限公司	268	0
北京天融信网络安全技术有限公司	256	12
新华三技术有限公司	158	0
华为技术有限公司	148	0
深信服科技股份有限公司	82	0
北京启明星辰信息安全技术有限公司	75	8
北京神州绿盟科技有限公司	49	12
北京奇虎科技有限公司	27	12
北京数字观星科技有限公司	20	0
北京知道创宇信息技术股份有限公司	6	4
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
远江盛邦（北京）网络安全科技股份有限公司	45	45
北京华云安信息技术有限公司	34	34

河南灵创电子科技有限公司	24	24
吉林谛听信息技术有限公司	17	17
杭州迪普科技股份有限公司	13	0
山东云天安全技术有限公司	6	6
济南三泽信息安全测评有限公司	5	5
广州竞远安全技术股份有限公司	5	5
南京众智维信息科技有限公司	5	5
山东道普测评技术有限公司	4	4
河北华测信息技术有限公司	3	3
内蒙古奥创科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
北京智游网安科技有限公司	1	1
安徽长泰信息安全服务有限公司	1	1
上海纽盾科技股份有限公司	1	1
京东云安全	1	1
北京浩瀚深度信息技术股份有限公司	1	1
北京顶象技术有限公司	1	1
北京神荼科技有限公司	1	1
CNCERT 四川分中心	2	2
CNCERT 西藏分中心	1	1
个人	478	478
报送总计	5057	3718

本周漏洞按类型和厂商统计

本周，CNVD 收录了 483 个漏洞。WEB 应用 171 个，应用程序 165 个，操作系统 110 个，网络设备（交换机、路由器等网络端设备）29 个，智能设备（物联网终端设备）6 个，安全产品 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	171
应用程序	165
操作系统	110
网络设备（交换机、路由器等网络端设备）	29
智能设备（物联网终端设备）	6
安全产品	2

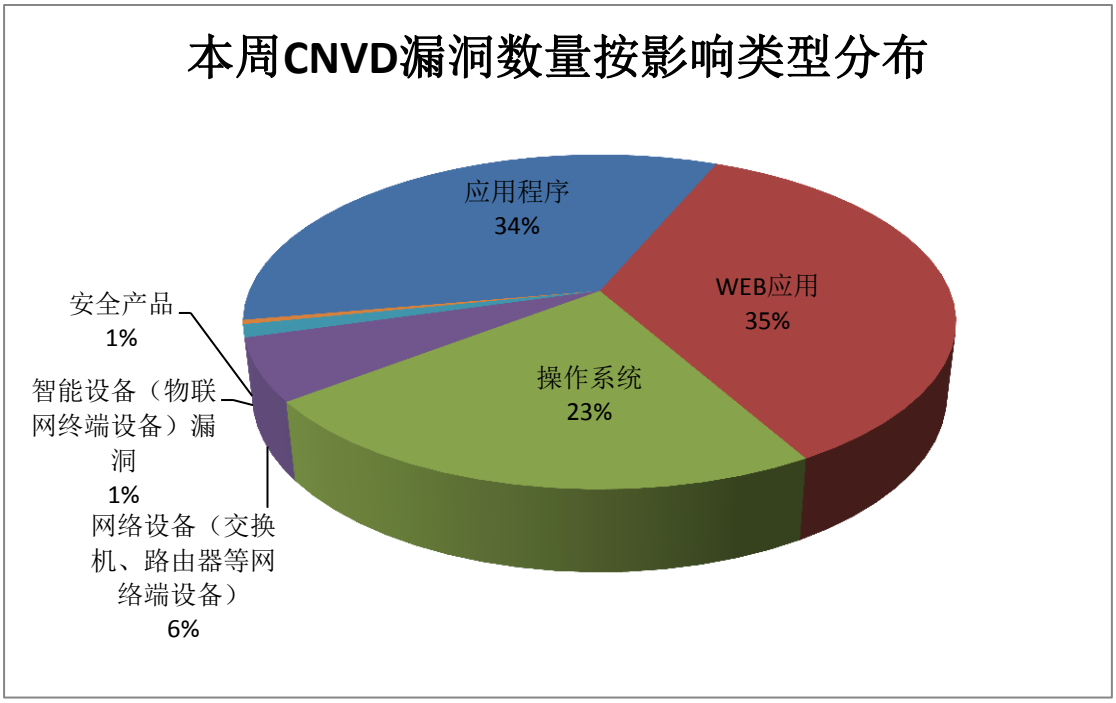

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、CloudBees 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	67	14%
2	Microsoft	26	5%
3	CloudBees	23	5%

4	kkcms	17	4%
5	IBM	15	3%
6	Cisco	12	2%
7	D-Link	10	2%
8	Apple	9	2%
9	WordPress	8	2%
10	其他	296	61%

本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，86 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，“Google Android System 权限提升漏洞（CNVD-2020-33230）、多款 Cisco 产品缓冲区溢出漏洞、D-Link DIR-865L 操作系统命令注入漏洞、多款 Apple 产品 Kernel 组件资源管理错误漏洞（CNVD-2020-33215）、Schneider Electric EcoStruxure Machine Expert - Basic 或 SoMachine Basic 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/

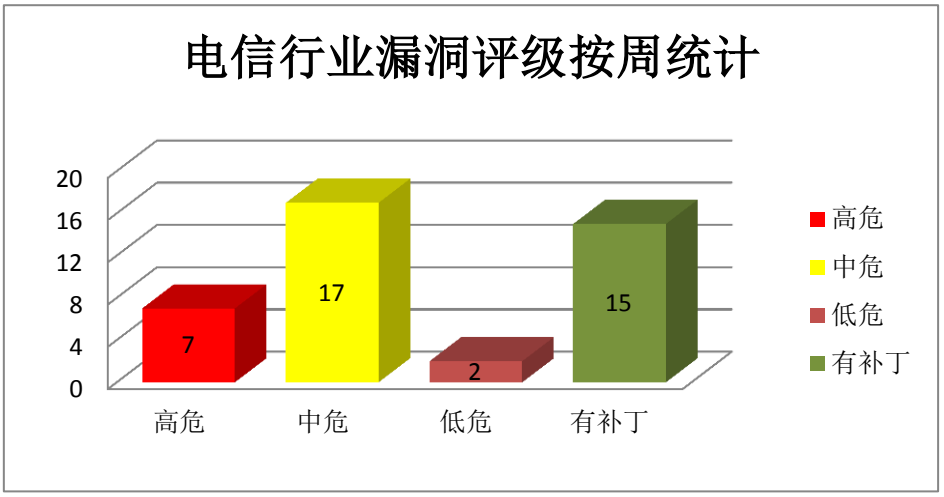

图 3 电信行业漏洞统计

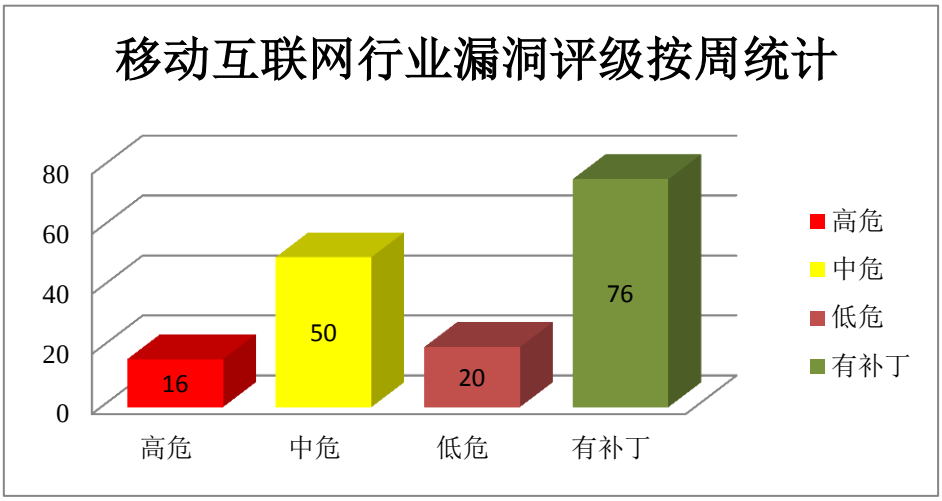

图 4 移动互联网行业漏洞统计

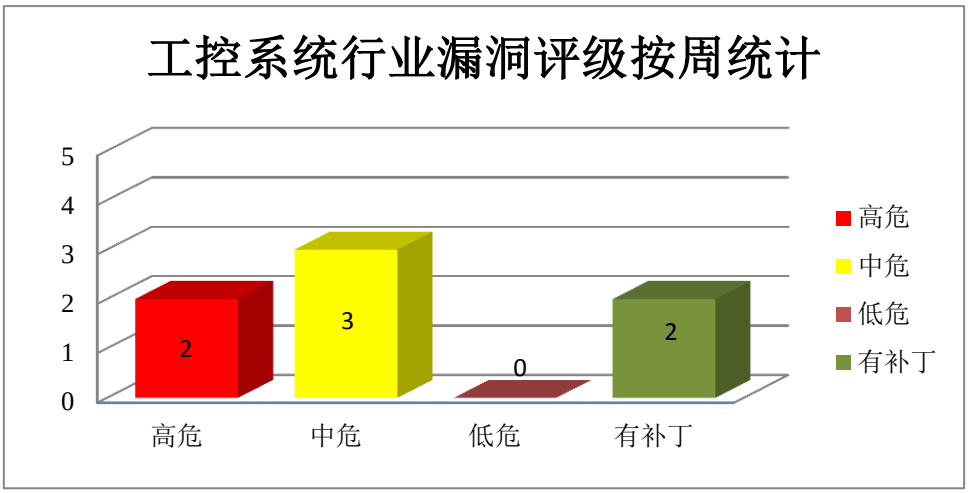

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Go 是的一款静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。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。System 是其中的一个系统组件。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敏感信息，提升权限，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android System 组件权限提升漏洞（CNVD-2020-32918、CNVD-2020-32920、CNVD-2020-32919）、Google Android System 组件信息泄露漏洞（CNVD-2020-32923、CNVD-2020-32922）、Google Android System 缓冲区溢出漏洞（CNVD-2020-33221）、Google Android System 权限提升漏洞（CNVD-2020-

33230）、Google Go 信任管理问题漏洞（CNVD-2020-33729）。其中，“Google Android System 缓冲区溢出漏洞（CNVD-2020-33221）、Google Android System 权限提升漏洞（CNVD-2020-33230）、Google Go 信任管理问题漏洞（CNVD-2020-33729）”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-2020-32918
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32920
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32919
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32923
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32922
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33221
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33230
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33729

2、Microsoft 产品安全漏洞

Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Windows Jet Database Engine 是其中的一个数据库引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致目标系统停止响应。

CNVD 收录的相关漏洞包括：Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2020-33077、CNVD-2020-33432、CNVD-2020-33431、CNVD-2020-33430）、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2020-33422、CNVD-2020-33421、CNVD-2020-33433）、Microsoft Windows 和 Windows Server 拒绝服务漏洞（CNVD-2020-33424）。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-2020-33077
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33422
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33421
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33424
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33432
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33431
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33430
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33433

3、Cisco 产品安全漏洞

Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco IOS 是一套为其网络设备开发的操作系统。IOS XE 是一套为其网络设备开发的操作系统。Cisco

809 Industrial Integrated Services Routers 是一款工业集成多业务路由器。Cisco 1000 Series Connected Grid Routers 是一款 1000 系列互联网格路由器。Cisco ASR 920 Series Aggregation Services Router ASR920-12SZ-IM 是美国思科（Cisco）公司的一款 920 系列聚合服务路由器。Cisco Content Security Management Appliance 是一套内容安全管理设备。该设备主要用于管理电子邮件和 Web 安全设备的所有策略、报告、审计信息等。AsyncOS Software 是运行在其中的一套操作系统。Cisco Application Services Engine 是美国思科（Cisco）公司的一套用于部署 Cisco 数据中心应用的通用平台。Cisco Wireless LAN Controller（WLC）Software 是美国思科（Cisco）公司的一套用于配置和管理 WLC（无线局域网控制器）的软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Cisco 产品输入验证错误漏洞（CNVD-2020-32900）、多款 Cisco 产品缓冲区溢出漏洞、Cisco ASR 920 Series Aggregation Services Router ASR920-12SZ-IM 代码问题漏洞、Cisco IOS 和 IOS XE 输入验证错误漏洞（CNVD-2020-32903）、多款 Cisco 产品 AsyncOS 输入验证错误漏洞、Cisco Application Services Engine 访问控制错误漏洞（CNVD-2020-32907）、Cisco Wireless LAN Controller Software 缓冲区溢出漏洞、Cisco Wireless LAN Controller Software 输入验证错误漏洞（CNVD-2020-33644）。其中，“多款 Cisco 产品输入验证错误漏洞（CNVD-2020-32900）、多款 Cisco 产品缓冲区溢出漏洞、Cisco IOS 和 IOS XE 输入验证错误漏洞（CNVD-2020-32903）”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-2020-32900
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32906
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32905
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32903
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32909
https://www.cnvd.org.cn/flaw/show/CNVD-2020-32907
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33645
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33644

4、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。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，执行任意命令等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins Selenium Plugin 跨站请求伪造漏洞、CloudBees Jenkins Play Framework Plugin 操作系统命令注入漏洞、CloudBees Jenkins Copy Artifact Plugin 授权问题漏洞、CloudBees Jenkins SCM Filter Jervis Plugin

代码问题漏洞、CloudBees Jenkins Amazon EC2 Plugin 授权问题漏洞、CloudBees Jenkins Amazon EC2 Plugin 信任管理问题漏洞、CloudBees Jenkins Amazon EC2 Plugin 跨站请求伪造漏洞、CloudBees Jenkins Copr Plugin 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-2020-33744
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33748
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33751
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33757
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33756
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33755
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33754
https://www.cnvd.org.cn/flaw/show/CNVD-2020-33758

5、TRENDnet TEW-827DRU 命令注入漏洞（CNVD-2020-33483）

TRENDnet TEW-827DRU 是一款无线路由器。本周，TRENDnet TEW-827DRU 被披露存在命令注入漏洞。攻击者可利用该漏洞在设备上运行任意命令。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-2020-33483

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-2020-32916	Artica Pandora FMS 权限提升漏洞	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://pandorafms.org/
CNVD-2020-33143	多款 IBM 产品缓冲区溢出漏洞（CNVD-2020-33143）	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.ibm.com/support/pages/node/6221324
CNVD-2020-33148	PHP 输入验证错误漏洞（CNVD-2020-33148）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugs.php.net/bug.php?id=78875
CNVD-2020-33149	PHP 缓冲区溢出漏洞（CNVD-2020-33149）	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.ibm.com/support/pages/node/6208333
CNVD-2020-	D-Link DIR-865L 操作系统命	高	目前厂商已发布升级补丁以修复漏

33168	令注入漏洞		洞，补丁获取链接：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174
CNVD-2020-33249	Vesta Control Panel 权限提升漏洞	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://vestacp.com/
CNVD-2020-33330	HPE UIoT 未授权访问漏洞（CNVD-2020-33330）	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/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbhf03947en_us
CNVD-2020-33337	LibVNCServer 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/LibVNC/libvncserver/commit/54220248886b5001fbbb9fa73c4e1a2cb9413fed
CNVD-2020-33589	ALLE INFORMATION School Manage System SQL 注入漏洞	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.schoolsoft.com.tw/
CNVD-2020-33766	WordPress pricing-table-by-supsystic 不安全权限漏洞	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://cn.wordpress.org/plugins/pricing-table-by-supsystic/#developers

小结：本周，Google 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，造成拒绝服务。此外，Microsoft、Cisco、CloudBees 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，执行任意命令，造成拒绝服务等。另外，TRENDnet TEW-827DRU 被披露存在命令注入漏洞。攻击者可利用该漏洞在设备上运行任意命令。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、Cellebrite UFED 输入验证错误漏洞

验证描述

Cellebrite UFED 是以色列 Cellebrite 公司的一款通用取证产品。该产品主要用于设备的数据提取、传输和分析等。

Cellebrite UFED 5.0 版本至 7.5.0.845 版本中存在输入验证错误漏洞，攻击者可利用该漏洞绕过操作系统策略，获取命令窗口。

验证信息

POC 链接：https://packetstormsecurity.com/files/157715/Cellebrite-UFED-7.5.0.845-Desktop-Escape-Privilege-Escalation.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-33496

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. 79 种 Netgear 路由器模型中发现了未修补的漏洞

两名安全研究人员独立发现了一个新漏洞，该漏洞影响了多年来在 79 个 Netgear 路由器上使用的 758 个不同的固件版本，其中一些固件版本最早是在 2007 年发布的设备上部署的。另外，该漏洞可能使黑客远程接管设备。

参考链接：https://www.zdnet.com/article/unpatched-vulnerability-identified-in-79-netgear-router-models/

2. Ripple 20 0day 漏洞曝光，扫荡全球各行业数亿台联网设备

以色列网络安全公司 JSOF 周二警告说，由于严重安全漏洞影响了 Treck TCP/IP 堆栈，全球数亿台（甚至更多）IoT 设备可能会受到远程攻击。

参考链接：https://securityaffairs.co/wordpress/104846/hacking/ripple20-vulnerabilities.html

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