# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2020 年 04 月 27 日-2020 年 05 月 03 日　　2020 年第 18 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 374 个，其中高危漏洞 160 个、中危漏洞 194 个、低危漏洞 20 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“PHP-FPM 远程代码执行漏洞（CNVD-2020-25851）、WordPress Catch Breadcrumb 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 3232 个，与上周（5304 个）环比减少 39%。

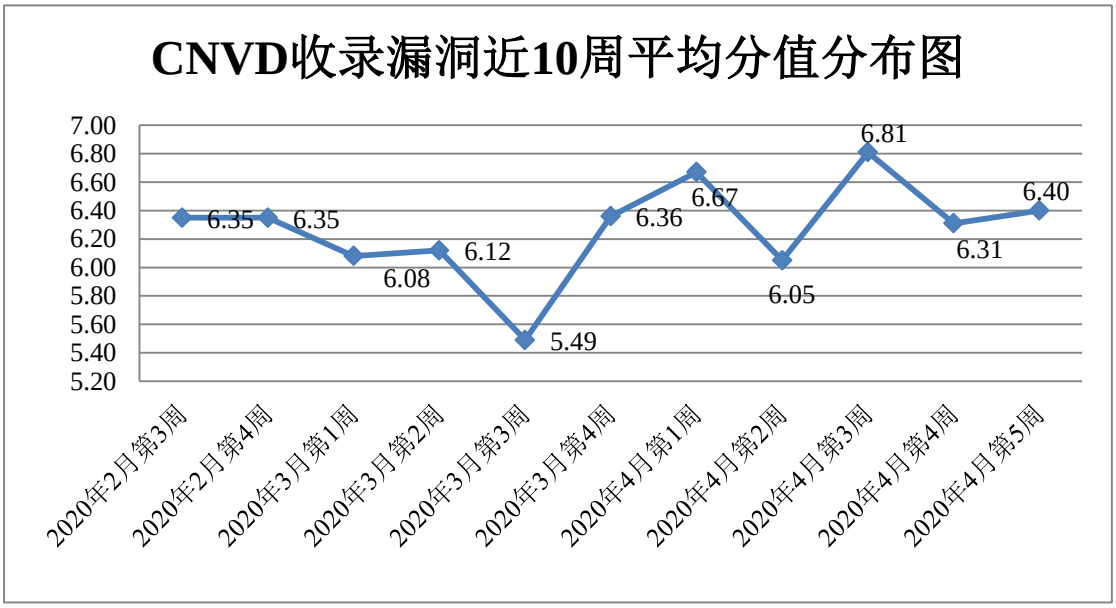


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 3 起，向基础电信企业通报漏洞事件 2 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 225 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 30 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：

深圳安远科技有限公司、上海银狐信息科技有限公司、河北欧润天腾科技发展有限公司、大庆久久网络科技有限公司、北京爱奇艺科技有限公司、深圳市圆梦云科技有限公司、深圳市微客互动有限公司、哈尔滨伟成科技有限公司、广州网易计算机系统有限公司、研华科技（中国）有限公司、横河电机(中国)有限公司、深圳市西迪特科技有限公司、洪湖尔创网联信息技术有限公司、三菱电机自动化（中国）有限公司、科大讯飞股份有限公司、广东凯格科技有限公司、上海宝信软件股份有限公司、北京金方时代科技有限公司、长沙米拓信息技术有限公司、安徽辛普信息科技有限公司、湖南翱云网络科技有限公司、赤峰易拓网络有限公司、长园深瑞继保自动化有限公司、潮州市微派网络科技有限公司、广东堡塔安全技术有限公司、深圳市显控科技股份有限公司、河北南昊高新技术开发有限公司、大庆紫金桥软件技术有限公司、河马软件有限责任公司、北京因酷时代科技有限公司、武汉创益云信息技术有限公司、上海金慧软件有限公司、山西先启科技有限公司、北京良精志诚科技有限责任公司、深圳市吉祥腾达科技有限公司、北京派网软件有限公司、北京映翰通网络技术股份有限公司、北京五指互联科技有限公司、浙江深大智能科技有限公司、南京汇微达信息技术有限公司、广东世纪信通网络科技有限公司、安科瑞电气股份有限公司、上海荃路软件开发工作室、贴心猫(imcat)、BEESCMS、Heybbs、SSYCMS、Yycms、YCCMS、115CMS 和 Advantech Co., Ltd.。

## 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、恒安嘉新(北京)科技股份公司、中新网络信息安全股份有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。北京铭图天成信息技术有限公司、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、远江盛邦（北京）网络安全科技股份有限公司、长春嘉诚信息技术股份有限公司、杭州迪普科技股份有限公司、国瑞数码零点实验室、杭州海康威视数字技术股份有限公司、京东云安全、山东云天安全技术有限公司、南方电网数字电网研究院有限公司、博智安全科技股份有限公司、河南信安世纪科技有限公司、成都安美勤信息技术股份有限公司、广州美杜莎网络科技有限公司及其他个人白帽子向 CNVD 提交了 3232 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 2250 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） | 1017 | 1017 |
| 斗象科技（漏洞盒子） | 787 | 787 |
| 上海交大 | 446 | 446 |
| 北京天融信网络安全技术有限公司 | 304 | 2 |
| 恒安嘉新(北京)科技股份公司 | 250 | 0 |
| 中新网络信息安全股份有限公司 | 206 | 206 |
| 哈尔滨安天科技集团股份有限公司 | 179 | 0 |
| 华为技术有限公司 | 159 | 0 |
| 深信服科技股份有限公司 | 143 | 0 |
| 四川无声信息技术有限公司 | 63 | 63 |
| 北京神州绿盟科技有限公司 | 60 | 1 |
| 中国电信集团系统集成有限责任公司 | 45 | 45 |
| 厦门服云信息科技有限公司 | 35 | 0 |
| 北京奇虎科技有限公司 | 24 | 15 |
| 内蒙古奥创科技有限公司 | 23 | 23 |
| 西安四叶草信息技术有限公司 | 15 | 15 |
| 北京启明星辰信息安全技术有限公司 | 7 | 7 |
| 新华三技术有限公司 | 3 | 0 |
| 北京知道创宇信息技术股份有限公司 | 3 | 0 |
| 杭州安恒信息技术股份有限公司 | 2 | 2 |
| 北京铭图天成信息技术有限公司 | 80 | 80 |

| | | |
|---|---|---|
| 北京华云安信息技术有限公司 | 40 | 40 |
| 河南灵创电子科技有限公司 | 36 | 36 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 33 | 33 |
| 长春嘉诚信息技术股份有限公司 | 31 | 31 |
| 杭州迪普科技股份有限公司 | 14 | 0 |
| 国瑞数码零点实验室 | 14 | 14 |
| 杭州海康威视数字技术股份有限公司 | 9 | 9 |
| 京东云安全 | 5 | 5 |
| 山东云天安全技术有限公司 | 3 | 3 |
| 南方电网数字电网研究院有限公司 | 2 | 2 |
| 博智安全科技股份有限公司 | 2 | 2 |
| 河南信安世纪科技有限公司 | 2 | 2 |
| 成都安美勤信息技术股份有限公司 | 1 | 1 |
| 广州美杜莎网络科技有限公司 | 1 | 1 |
| CNCERT 西藏分中心 | 10 | 10 |
| CNCERT 贵州分中心 | 5 | 5 |
| CNCERT 宁夏分中心 | 1 | 1 |
| 个人 | 328 | 328 |
| 报送总计 | 4388 | 3232 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 374 个漏洞。应用程序 190 个，WEB 应用 99 个，网络设备（交换机、路由器等网络端设备）61 个，操作系统 17 个，安全产品 4 个，数据库 2 个，智能设备（物联网终端设备）漏洞 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 | 190 |
| WEB 应用 | 99 |
| 网络设备（交换机、路由器等网络端设备） | 61 |
| 操作系统 | 17 |
| 安全产品 | 4 |
| 数据库 | 2 |
| 智能设备（物联网终端设备）漏洞 | 1 |

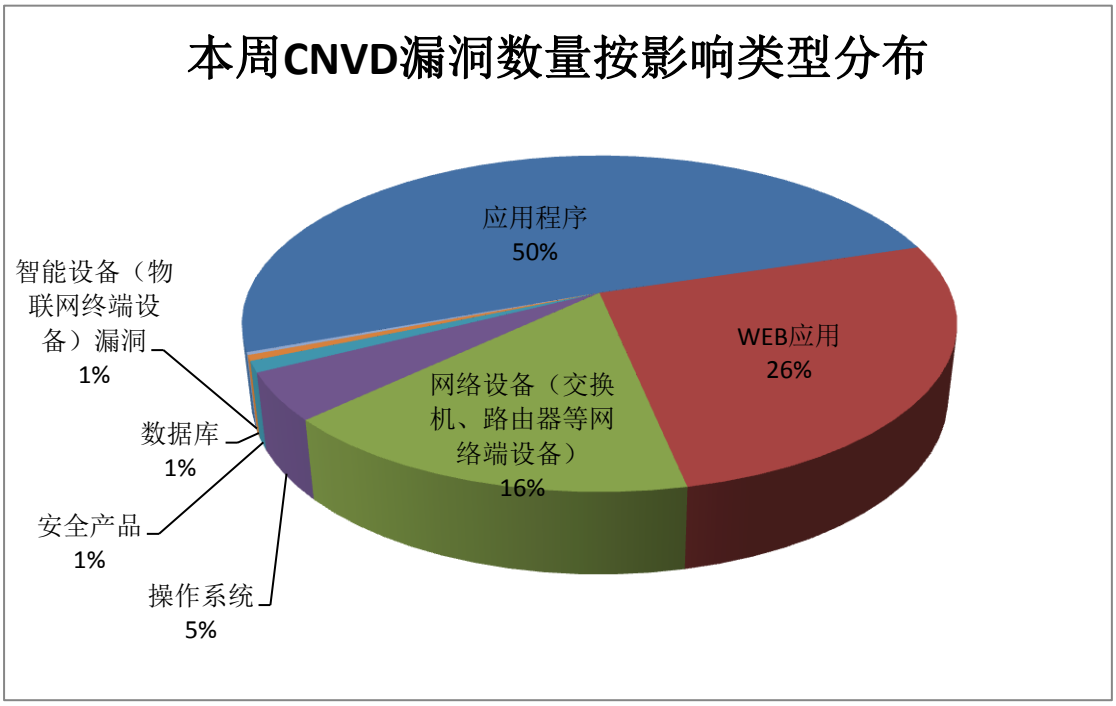


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 NETGEAR、Adobe、PrestaShop 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 | NETGEAR | 42 | 11% |
| 2 | Adobe | 21 | 6% |
| 3 | PrestaShop | 17 | 5% |
| 4 | Microsoft | 15 | 4% |
| 5 | Oracle | 13 | 3% |
| 6 | IBM | 11 | 3% |
| 7 | Cisco | 10 | 3% |

| | | | |
|---|---|---|---|
| 8 | Google | 8 | 2% |
| 9 | Broadcom | 8 | 2% |
| 10 | 其他 | 229 | 61% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 50 个电信行业漏洞，13 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Vertiv Avocent UMG-4000 Web 接口跨站脚本漏洞、Cisco Unified Communications Manager 和 Unified Communications Manager Session Management Edition 路径遍历漏洞、Synergy Systems & Solutions HUSKY RTU 6049-E70 访问控制错误漏洞、NETGEAR R7800 代码执行漏洞”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/

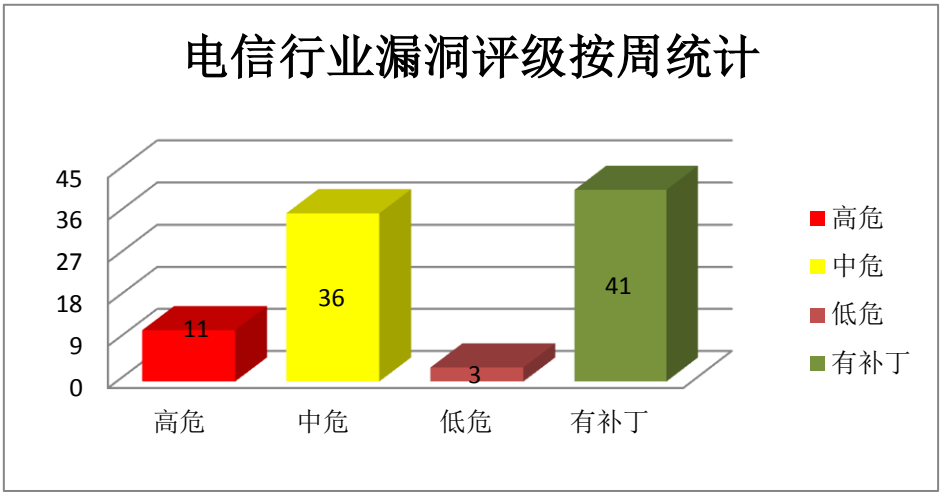


图 3 电信行业漏洞统计

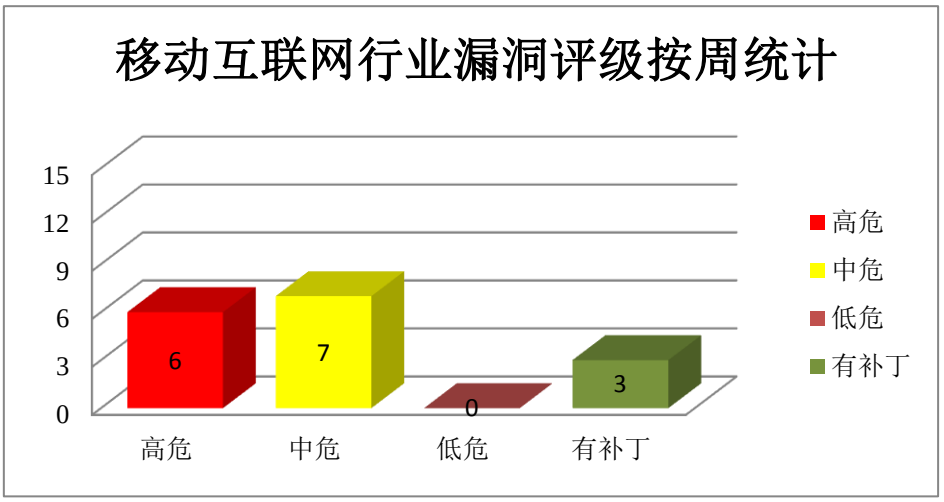

图 4 移动互联网行业漏洞统计

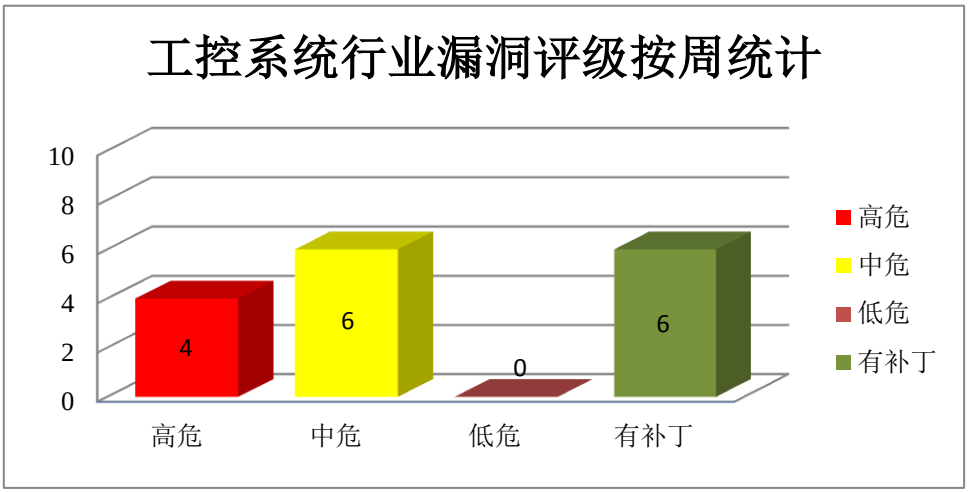


图 5 工控系统行业漏洞统计

## 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、Cisco 产品安全漏洞

Cisco UCS Director 和 Cisco UCS Director Express for Big Data 都是美国思科（Cisco）公司的产品。Cisco UCS Director 是一套私有云基础架构即服务（IaaS）的异构平台。Cisco UCS Director Express for Big Data 是一套针对大数据集群的基础架构统一管理平台。Cisco Webex Network Recording Player 和 Cisco Webex Network Webex Player 是一款用于播放视频会议记录的播放器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞写入任意文件，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco UCS Director 和 Cisco UCS Director Express for Big Data 输入验证错误漏洞（CNVD-2020-25346、CNVD-2020-25347）、Cisco Webex Network Recording Player 和 Webex Player 代码执行漏洞、Cisco UCS Director 和 Cisco UCS Director Express for Big Data 路径遍历漏洞（CNVD-2020-25345、CNVD-2020-25351、CNVD-2020-25349、CNVD-2020-25348、CNVD-2020-25350）。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-2020-25346

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25345

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25344

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25349

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25348

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25347

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25351

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25350

**2、IBM 产品安全漏洞**

IBM MaaS360 是美国 IBM 公司的一套企业移动设备管理解决方案。IBM Spectrum Protect（前称 Tivoli Storage Manager）是一套数据保护平台。IBM Tivoli Monitoring 是一套系统监控软件。IBM TRIRIGA Application Platform 是一套用于部署 TRIRIGA 应用的技术平台。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Automation Workstream Services in Cloud Pak for Automation 和 IBM Process Federation Server 是 IBM 工作流程自动化服务和 IBM 联合服务器。IBM Maximo Anywhere 是一套建立在 IBM Worklight 平台上的下一代移动解决方案。IBM Cognos Analytics 是一套商业智能软件。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敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM MaaS360 信息泄露漏洞、IBM Spectrum Protect 代码执行漏洞、IBM Tivoli Monitoring 未授权访问漏洞、IBM TRIRIGA Application Platform 信息泄露漏洞（CNVD-2020-25568）、IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2020-25565）、IBM Automation Workstream Services in Cloud Pak for Automation 和 IBM Process Federation Server 拒绝服务漏洞、IBM Maximo Anywhere 信息泄露漏洞（CNVD-2020-25795）、IBM Cognos Analytics 信息泄露漏洞（CNVD-2020-26252）。其中，“IBM Spectrum Protect 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-2020-25561

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25563

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25562

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25568

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25565

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25569

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25795

https://www.cnvd.org.cn/flaw/show/CNVD-2020-26252

**3、Microsoft 产品安全漏洞**

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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 Kernel 是其中的一个 Windows 系统内核。Windows Jet Database Engine 是其中的一个数据库引擎。Push Notification Service 是其中的一个推送通知服务。Media Foundation 是其中的一个多媒体应用库。本周，上述产品被披露存在

多个漏洞，攻击者可利用漏洞提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows Kernel 提权漏洞（CNVD-2020-25579、CNVD-2020-25578、CNVD-2020-25583）、Microsoft Windows Jet Database Engine 代码执行漏洞、Microsoft Windows Push Notification Service 提权漏洞、Microsoft Windows Media Foundation 缓冲区溢出漏洞（CNVD-2020-26242、CNVD-2020-26244、CNVD-2020-26243）。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-2020-25579

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25578

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25577

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25581

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25583

https://www.cnvd.org.cn/flaw/show/CNVD-2020-26242

https://www.cnvd.org.cn/flaw/show/CNVD-2020-26244

https://www.cnvd.org.cn/flaw/show/CNVD-2020-26243

### 4、Adobe 产品安全漏洞

Adobe Bridge 是 Adobe 公司推出的一款免费数字资产管理应用程序。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-2020-25758、CNVD-2020-25761、CNVD-2020-25760、CNVD-2020-25790、CNVD-2020-25793、CNVD-2020-25792、CNVD-2020-25791）、Adobe Bridge 内存破坏漏洞。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-2020-25758

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25761

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25760

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25765

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25790

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25793

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25792

https://www.cnvd.org.cn/flaw/show/CNVD-2020-25791

### 5、Evenroute IQrouter 日志信息泄露漏洞

Evenroute IQrouter 是美国 Evenroute 公司的一款智能路由器。本周，Evenroute IQrouter 3.3.1 及之前版本被披露存在日志信息泄露漏洞。远程攻击者可利用该漏洞读取系统日志。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-2020-25370

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-2020-25376 | Synergy Systems & Solutions HUSKY RTU 6049-E70 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://www.s3india.com/ |
| CNVD-2020-25377 | NETGEAR R780 代码执行漏洞 | 高 | 厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：https://kb.netgear.com/000061740/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-R7800-PSV-2019-0076 |
| CNVD-2020-25532 | Oracle Virtualization VM VirtualBox 拒绝服务漏洞（CNVD-2020-25532） | 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.oracle.com/security-alerts/cpuapr2020.html |
| CNVD-2020-25573 | ThinkPHP 存在 SQL 注入漏洞（CNVD-2020-25573） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：http://www.thinkphp.cn/ |
| CNVD-2020-25812 | Ascensio System ONLYOFFICE Document Server SQL 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://github.com/ONLYOFFICE/DocumentServer/blob/master/CHANGELOG.md#551 |
| CNVD-2020-25814 | DAViCal Andrew’s Web Libraries 授权问题漏洞 | 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.davical.org/ |
| CNVD-2020-25836 | TP-Link TL-WA855RE login.json 身份验证权限提升不当漏洞 | 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.tp-link.com/ |
| CNVD-2020-25869 | Xen 拒绝服务漏洞（CNVD-2020-25869） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://xenbits.xen.org/xsa/advisory-314.html |
| CNVD-2020-25877 | Centreon 信息泄露漏洞 | 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.centreon.com/ |
| CNVD-2020-25980 | SAP Landscape Management 权限提升漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： |

| | | | |
|---|---|---|---|
| | | | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=544214202 |

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞写入任意文件，执行任意代码，导致拒绝服务。此外 IBM、Microsoft、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞攻击者可利用漏洞获取敏感信息、执行任意代码，导致拒绝服务。另外，Evenroute IQrouter 3.3.1 及之前版本被披露存在日志信息泄露漏洞。远程攻击者可利用该漏洞读取系统日志。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、WordPress Catch Breadcrumb 跨站脚本漏洞

**验证描述**

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Catch Breadcrumb 是使用在其中的一个面包屑导航插件，它主要用于显示目前所处的网页位置。

WordPress Catch Breadcrumb 1.5.4 之前版本中存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

**验证信息**

POC 链接：https://cxsecurity.com/issue/WLB-2020040144

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-25585

**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. 专家发布 OpenSSL 中的 DoS 漏洞 CVE-2020-1967

最近，OpenSSL 项目发布了针对 OpenSSL 的安全更新，该更新修补了一个高危漏洞，跟踪为 CVE-2020-1967，攻击者可以利用该漏洞发起拒绝服务（DoS）攻击。

参考链接：https://securityaffairs.co/wordpress/102763/hacking/cve-2020-1967-dos-openssl-exploit.html

### 2. WordPress 5.4.1 发布 修复 7 个安全漏洞和多个问题

WordPress 5.4.1 已经发布，并且正式推送更新。该版本除了修复了 7 个安全漏洞外，还修复了 17 个错误，建议大家尽快更新。此外，自 WordPress 3.7 以来的所有版本也已更新了对应的子版本。

参考链接：https://www.cnbeta.com/articles/soft/974251.htm

## 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