国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 04 月 01 日-2019 年 04 月 07 日 **2019 年第 14 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 180 个，其中高危漏洞 71 个、中危漏洞 78 个、低危漏洞 31 个。漏洞平均分值为 5.99。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 47%），其中互联网上出现“BigTree CMS 'parent' SQL 注入漏洞、WordPress 插件 WordPress-Feed-Statistics 开放重定向漏洞”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 1599 与上周（1960 个）环比下降 18%。

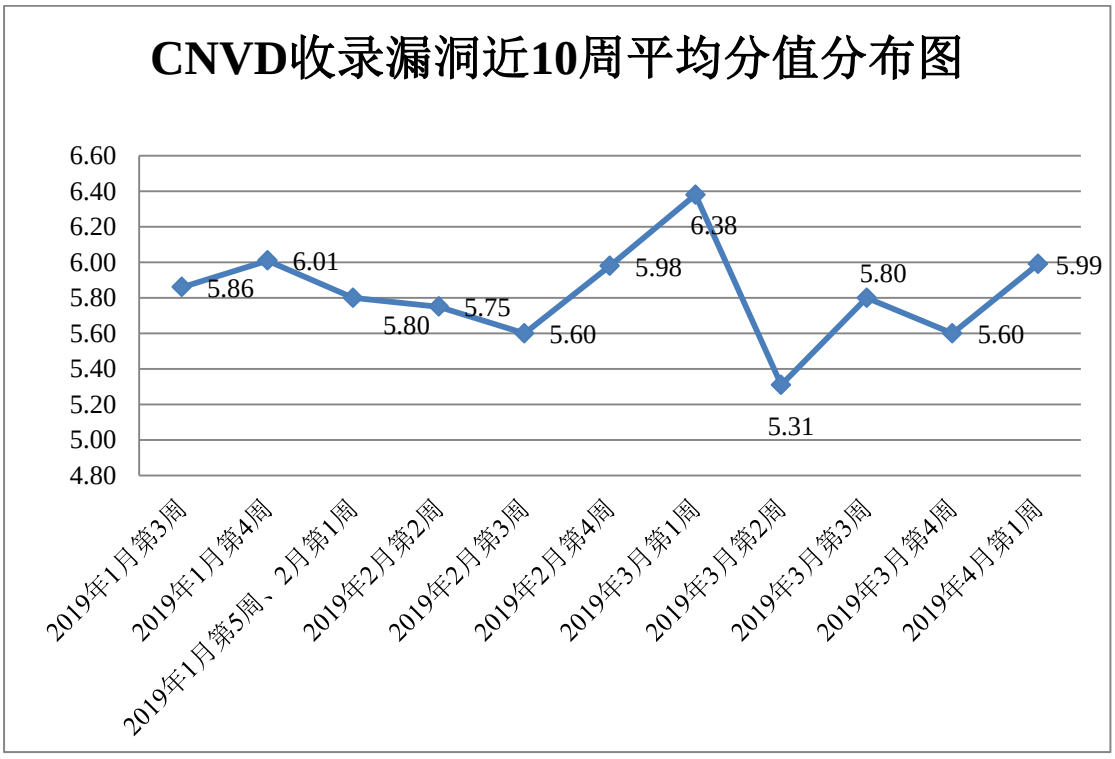

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 3 起，向银行、保险、能源等重要行业

单位通报漏洞事件 10 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 273 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 25 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：

SeaCMS、XnView、北京通达信科科技有限公司、中国美术协会网、北京小米科技有限责任公司、Joomla、中国节能环保集团有限公司、深圳市锟铻科技有限公司、Jfinal、cms、合优网络、中国船舶重工集团有限公司、北京广研广播电视高科技中心、海洋 CMS、昆明市网翼通科技有限公司、财通证券资产管理有限公司、魅思网络科技有限公司、中国土地市场网、Z-Blog、宁波易龙（橄榄树）计算机科技有限公司、福建福昕软件开发股份有限公司、中国电子制造人才网、中国少年预备役训练营和期货日报网。

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、深信服科技股份有限公司、四川无声信息技术有限公司、华为技术有限公司、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。长春嘉诚信息技术股份有限公司、国瑞数码零点实验室、安徽锋刃信息科技有限公司、中新网络信息安全股份有限公司、北京圣博润高新技术股份有限公司、山东云天安全技术有限公司、河北华测信息技术有限公司、河南信安世纪科技有限公司、内蒙古奥创科技有限公司、江苏通付盾信息安全技术有限公司、山东华鲁科技发展股份有限公司、山石网科通信技术股份有限公司、安徽长泰信息安全服务有限公司、上海物盾信息科技有限公司、浙江鹏信信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 1599 事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1093 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）	667	667
360 网神（补天平台）	426	426
哈尔滨安天科技集团股份有限公司	200	0
深信服科技股份有限公司	105	0
四川无声信息技术有限公司	76	76

华为技术有限公司	76	0
恒安嘉新(北京)科技股份公司	57	57
北京启明星辰信息安全技术有限公司	56	5
北京天融信网络安全技术有限公司	47	2
新华三技术有限公司	47	0
北京神州绿盟科技有限公司	45	0
中国电信集团系统集成有限责任公司	45	0
北京数字观星科技有限公司	40	0
北京知道创宇信息技术有限公司	7	6
长春嘉诚信息技术股份有限公司	50	50
国瑞数码零点实验室	42	42
安徽锋刃信息科技有限公司	41	41
中新网络信息安全股份有限公司	37	37
北京圣博润高新技术股份有限公司	19	19
山东云天安全技术有限公司	15	15
河北华测信息技术有限公司	5	5
河南信安世纪科技有限公司	3	3
内蒙古奥创科技有限公司	3	3
江苏通付盾信息安全技术有限公司	2	2
山东华鲁科技发展股份有限公司	2	2
山石网科通信技术股份有限公司	1	1
安徽长泰信息安全服务有限公司	1	1

上海物盾信息科技有限公司	1	1
浙江鹏信信息科技股份有限公司	1	1
CNCERT 吉林分中心	10	10
CNCERT 贵州分中心	3	3
CNCERT 河南分中心	1	1
CNCERT 江苏分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 宁夏分中心	1	1
个人	120	120
报送总计	2254	1599

本周漏洞按类型和厂商统计

本周，CNVD 收录了 180 洞。应用程序漏洞 106 个，WEB 应用漏洞 45 个，操作系统漏洞 14 个，网络设备漏洞 14 个，安全产品漏洞 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
应用程序漏洞	106
WEB 应用漏洞	45
操作系统漏洞	14
网络设备漏洞	14
安全产品漏洞	1

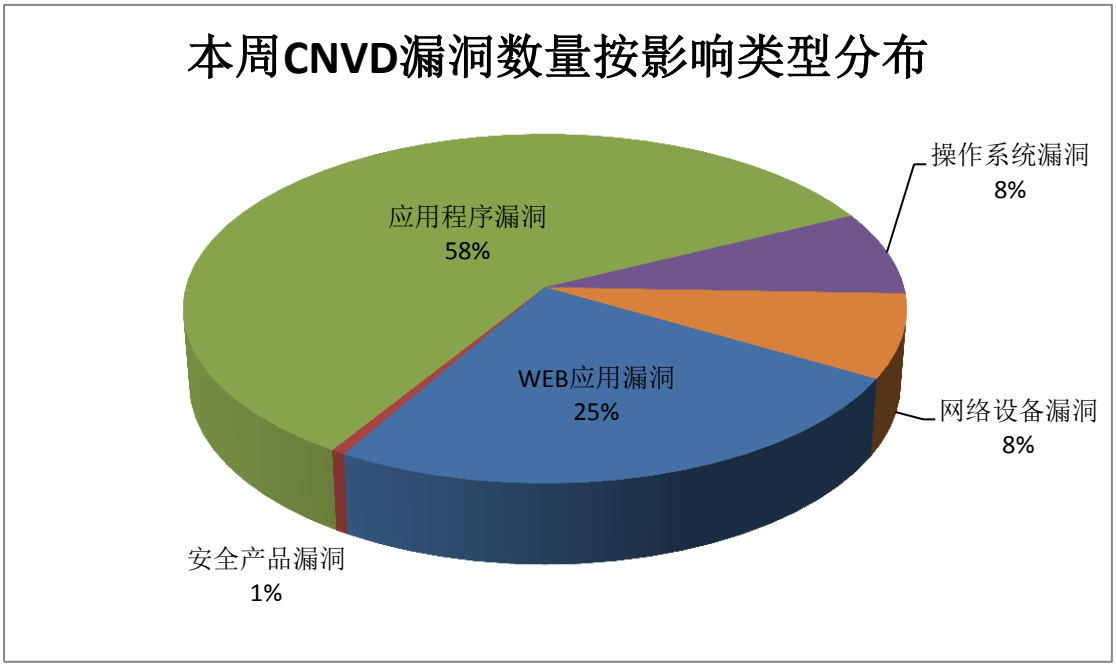

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Synology、Apache 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	Adobe	12	7%
2	Synology	12	7%
3	Apache	11	6%
4	CloudBees	9	5%
5	Google	9	5%
6	Poppler	6	3%
7	tiantiCMS	5	3%
8	IBM	4	2%
9	Libav	4	2%
10	其他	108	60%

本周行业漏洞收录情况

本周，CNVD 收录了 11 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，“Advantech WebAccess/SCADA 缓冲区溢出漏洞、Synology Router Manager 命令注入漏洞（CNVD-2019-08959）、Dell Networking OS10 密钥管理错

误漏洞、IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2019-09065）、ENTTEC Datagate MK2、Storm 24 和 Pixelator 拒绝服务漏洞”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，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/

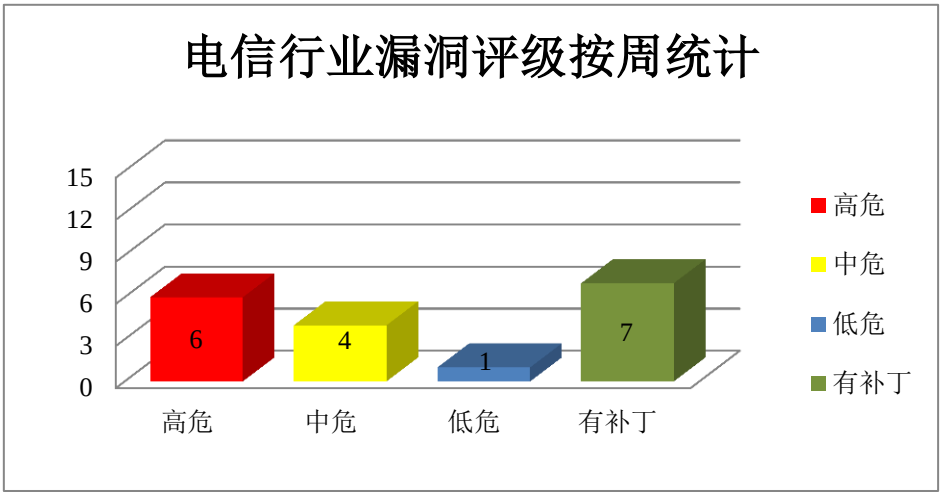

图 3 电信行业漏洞统计

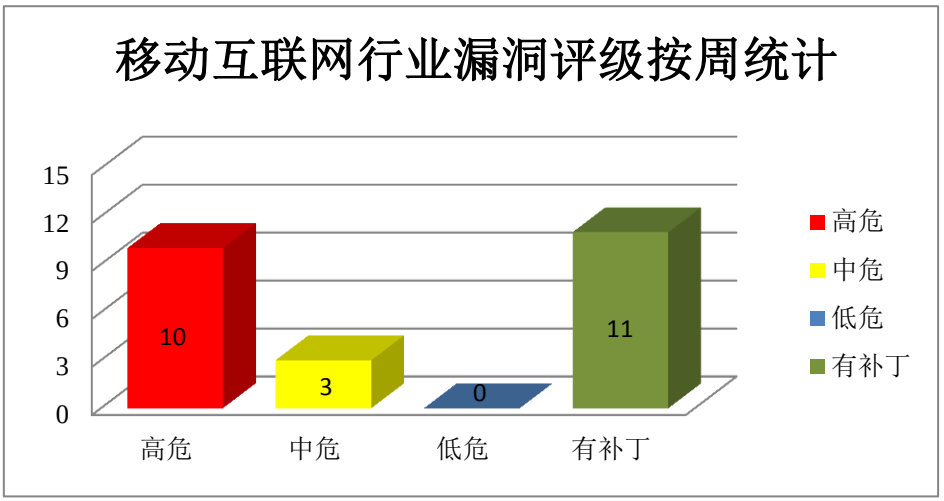

图 4 移动互联网行业漏洞统计

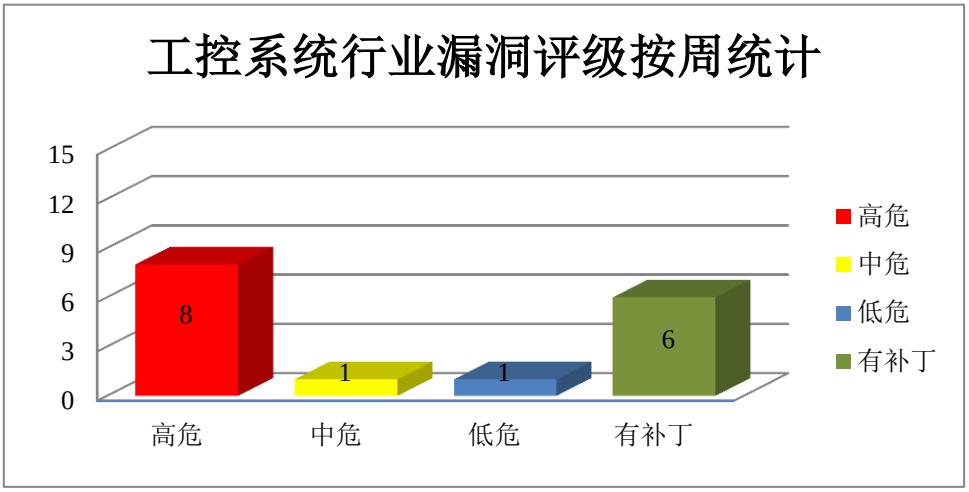

图 5 控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在内存错误引用漏洞，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 Acrobat 和 Reader 内存错误引用漏洞（CNVD-2019-09057、CNVD-2019-09058、CNVD-2019-09060、CNVD-2019-09059、CNVD-2019-09061、CNVD-2019-09063、CNVD-2019-09062、CNVD-2019-09064）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-09057

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09058

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09060

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09059

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09061

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09063

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09062

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09064

2、Synology 产品安全漏洞

Synology Router Manager（SRM）是一款用于配置和管理 Synology 路由器的软件。Synology File Station 是一套文件管理工具。Synology DiskStation Manager（DSM）是一套用于网络储存服务器（NAS）上的操作系统。Synology Application Service 是一款

Synology NAS（网络存储服务器）功能扩展框架。Synology Drive 是一套协同办公套件。本周，上述产品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。

CNVD 收录的相关漏洞包括：Synology Router Manager 信息泄露漏洞（CNVD-2019-08958、CNVD-2019-08961、CNVD-2019-08962）、Synology File Station 信息泄露漏洞、Synology DiskStation Manager 信息泄露漏洞（CNVD-2019-08960）、Synology Application Service 信息泄露漏洞（CNVD-2019-08965、CNVD-2019-08967）、Synology Drive 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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08958

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08957

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08960

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08961

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08962

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08965

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08964

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08967

3、Apache 产品安全漏洞

Apache HTTP Server 是一款开源网页服务器。Apache httpd 是一款专为现代操作系统开发和维护的开源 HTTP 服务器。Apache Jmeter 是一套使用 Java 语言编写的用于压力测试和性能测试的开源软件。Apache JSPWiki 是一款基于 Java、Servlet 和 JSP 构建的开源 WikiWiki 引擎。Apache ActiveMQ 是一套开源的消息中间件，它支持 Java 消息服务、集群、Spring Framework 等。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，绕过身份验证机制并执行未经授权的操作，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apache httpd 安全绕过漏洞（CNVD-2019-08942）、Apache HTTP Server 访问绕过漏洞、Apache httpd 安全绕过漏洞、Apache HTTP Server 本地权限提升漏洞、Apache HTTP Server 身份验证绕过漏洞、Apache Jmeter 远程代码执行漏洞、Apache JSPWiki 信息泄露漏洞、Apache ActiveMQ 拒绝服务漏洞（CNVD-2019-09281）。其中，除“Apache httpd 安全绕过漏洞、Apache ActiveMQ 拒绝服务漏洞（CNVD-2019-09281）” 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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08942

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08944

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08943

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08946

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08945

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08982

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09279

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09281

4、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是一套基于 Java 开发的持续集成工具。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒保护，捕获存储在 Jenkins 中的凭证，执行未授权的操作，并在 Web 页面中注入任意的 JavaScript 代码等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins 沙盒绕过漏洞（CNVD-2019-09287、CNVD-2019-09291）、CloudBees Jenkins CSRF 漏洞、CloudBees Jenkins 跨站请求伪造漏洞（CNVD-2019-09290、CNVD-2019-09294）、CloudBees Jenkins 跨站脚本漏洞（CNVD-2019-09292）、CloudBees Jenkins 信息泄露漏洞（CNVD-2019-09293）、CloudBees Jenkins SSRF 漏洞。其中，“CloudBees Jenkins 沙盒绕过漏洞（CNVD-2019-09287、CNVD-2019-09291）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-09287

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09288

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09290

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09292

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09291

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09294

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09293

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09295

5、Red Hat OpenShift OAuth server 跨站脚本漏洞

Red Hat OpenShift 是美国红帽（Red Hat）公司的一款平台即服务（PaaS）云计算平台，它支持构建、测试、部署和运行应用程序。OAuth server 是其中的一个 OAuth（开放授权）服务器。Red Hat OpenShift OAuth server 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08972

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-2019-08856	VMware Fusion 虚拟机端远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.vmware.com/cn/products/fusion/fusion-evaluation.html
CNVD-2019-08948	Advantech WebAccess/SCADA 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://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download
CNVD-2019-08969	ENTTEC Datagate MK2、Storm 24 和 Pixelator 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.enttec.com/product/controls/dmx-ethernet-lighting-control/advanced-lighting-data-control/
CNVD-2019-08981	多款 Qualcomm 产品访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2019-03-01.html
CNVD-2019-09046	Phusion Passenger SpawningKit 存在多个漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://blog.phusion.nl/2018/06/12/passenger-5-3-2-various-security-fixes/
CNVD-2019-09065	IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2019-09065）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10875692
CNVD-2019-09132	Sourcetree for macOS 参数注入漏洞（CNVD-2019-09132）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcetreeapp.com/
CNVD-2019-09276	NetGain Enterprise Manager 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：http://www.netgain-systems.com/netgain-enterprise-manager/
CNVD-2019-09280	ARC 和 Rockwell Automation PowerFlex 525 资源消耗漏洞	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.rockwellautomation.com
CNVD-2019-09286	Dell Networking OS10 密钥管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/article/SLN316558/

小结：本周，Adobe 被披露存在内存错误引用漏洞，攻击者可利用漏洞执行任意代码。此外，Synology、Apache、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，绕过身份验证机制并执行未经授权的操作，发起拒绝服务攻击，并在 Web 页面中注入任意的 JavaScript 代码等。另外，Red Hat OpenShift OAuth server 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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、BigTree CMS 'parent' SQL 注入漏洞

验证描述

BigTree CMS 是一个基于 PHP 和 MySQL 的开源内容管理系统。

BigTree CMS 'parent'存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=32678

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08953

信息提供者

CNVD 工作组

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. 黑客滥用 Google Cloud 攻击 D-Link 路由器

一位研究人员表示，在过去三个月中，谷歌云平台遭到滥用，针对 D-Link、ARGtek、DSLink、Secutech 和 TOTOLINK 路由器进行三次 DNS 劫持攻击，DNS 劫持会导致路由器流量被重定向并发送到恶意网站。2018 年 12 月 29 日，第一波攻击发起，目标是 D-Link DSL-2640B、D-Link DSL-2740R、D-Link DSL-2780B 和 D-Link DSL-526B，将其重定向到加拿大的流氓 DNS 服务器。2019 年 2 月 6 日发起的第二波攻击也针对这些相同类型的 D-Link 调制解调器。3 月 26 日，第三次攻击是针对的是 ARG-W4 ADSL 、DSLink 260E、Secutech 和 TOTOLINK 的路由器。虽然暂时无法列出有多少路由器受到其影响，但有研究者表示，超过 14000 台 D-Link DSL-2640B 路由器与 2265 台 TOTOLINK 路由器暴露在公网上。研究人员也没有具体说明攻击者如何攻击路由器。

参考链接：https://www.leiphone.com/news/201904/TGFdmEvQcy2A0ks8.html

2. WordPress iOS 应用程序泄露身份验证令牌

WordPress 官方 iOS 应用程序中出现一个漏洞，这个漏洞可能会将用户的帐户身份验证令牌暴露给第三方网站。这个问题主要影响到一些外部托管图像的私人网站（如 Flicker 等），这些网站可以通过 WordPress 应用程序查看或编写。WordPress 母公司 Automattic 公司表示目前没有用户名和密码泄露，只是泄露了应用程序与 WordPress.com 之

间通信和认证的“安全”令牌。这意味着，如果用户使用 WordPress iOS 应用创建或编辑包含托管在第三方网站上的图像的博客，则第三方网站可能会意外收到 WordPress.com 安全令牌。目前，该漏洞已经修复。

参考链接：https://www.zdnet.com/article/wordpress-ios-app-leaked-authentication-tokens/

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