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 15 日-2019 年 04 月 21 日 **2019 年第 16 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 230 个，其中高危漏洞 96 个、中危漏洞 115 个、低危漏洞 19 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 122 个（占 53%），其中互联网上出现“Apache Axis 代码执行漏洞、QCMS 跨站请求伪造漏洞”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 1994 与上周（1755 个）环比增长 14%。

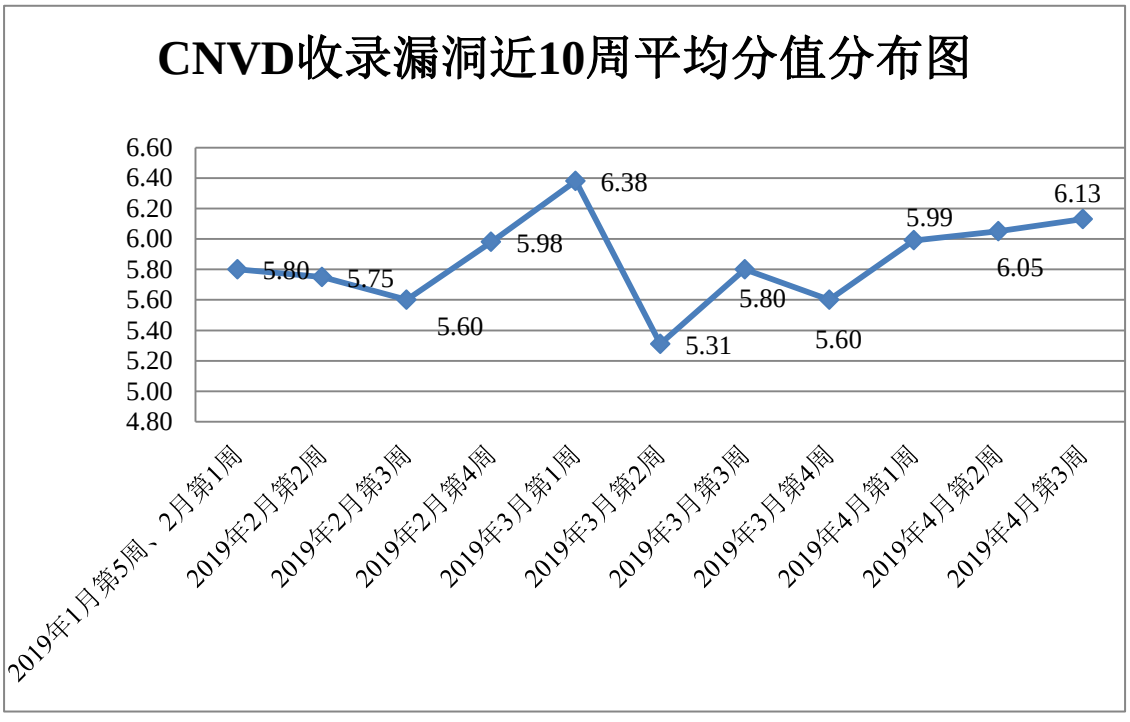

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 起，向银行、保险、能源等重要行业单位通报漏洞事件 38 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 563 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 51 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：

广州齐博网络科技有限公司、安徽华易网络科技有限公司、北京火绒网络科技有限公司、中国建材检验认证集团股份有限公司、黑龙江艺通网络技术开发有限公司、宁波海曙橄榄树计算机科技有限公司、洪湖尔创网联信息技术有限公司、苏州烟火网络科技有限公司、北京动网天下科技有限公司、苏州烟火网络科技有限公司、北京动网天下科技有限公司、上海汉得信息技术股份有限公司、中国大唐集团科学技术研究院有限公司、深圳神州通达网络技术有限公司、山东城通科技有限公司、重庆远秋科技公司、江苏鑫跃科技有限公司、沧州市凡诺广告传媒有限公司、灵宝简好网络科技有限公司、深圳同天下科技有限公司、淄博闪灵网络科技有限公司、上海茸易科技有限公司、深圳市锟锆科技有限公司、华宝证券有限责任公司、湖南潭州教育网络科技有限公司、宁波在线网络信息有限公司、上海五五来客科技股份有限公司、天气网、中国船舶报社、中国经济体制改革研究会、中国通信标准化协会、快范之家、厦门大学附属第一医院、中国建筑工业出版社、浙江深大智能集团、中国测试科技资讯平台、易企 CMS、DM 建站系统、爱客 CMS、鱼跃 CMS、Z-Blog、zzzcms、GraphicsMagick Group、phpwind、KUNBUS、SchoolCMS、iCMS、HadSky。

本周，CNVD 发布了《Oracle 发布 2019 年 2 月的安全公告》、《关于 Oracle WebLogic wls9-async 组件存在反序列化远程命令执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4987

http://www.cnvd.org.cn/webinfo/show/4989

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、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、华为技术有限公司、深信服科技股份有限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、国瑞数码安全系统股份有限公司（国瑞数码零点实验室）、中新网络信息安全股份有限公司、安徽锋刃信息科技有限公司、任子行网络技术股份有限公司、上海并擎软件科技有限公司、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、南京联成科技发展股份有限公司、山石网科通信技术股份有限公司、广州竞远安全技术股份有限公司、福建国科信息科技有限公司-漏斗社区、内蒙古奥创科技有限公司、北京信联科汇科技有限公司、成都安美勤信息技术股份有限公司、广州万方计算机科技有限公司、广州昊

达信息科技有限公司、广州思迈特软件有限公司、四川虹微技术有限公司（子午攻防实验室）及其他个人白帽子向 CNVD 提交了 1994 个以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 1354 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）	933	933
360 网神（补天平台）	421	421
新华三技术有限公司	252	0
哈尔滨安天科技集团股份有限公司	242	0
北京天融信网络安全技术有限公司	210	4
华为技术有限公司	139	0
深信服科技股份有限公司	85	0
北京启明星辰信息安全技术有限公司	79	0
恒安嘉新(北京)科技股份公司	43	0
北京神州绿盟科技有限公司	32	0
中国电信集团系统集成有限责任公司	28	0
北京数字观星科技有限公司	20	0
南京铱迅信息技术股份有限公司	8	0
北京知道创宇信息技术有限公司	6	0
厦门服云信息科技有限公司	5	0
长春嘉诚信息技术股份有限公司	176	176
国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	66	66
中新网络信息安全股份有	51	51

限公司		
安徽锋刃信息科技有限公司	39	39
任子行网络技术股份有限公司	34	34
上海并擎软件科技有限公司	28	28
北京圣博润高新技术股份有限公司	22	22
山东云天安全技术有限公司	21	21
南京联成科技发展股份有限公司	15	15
山石网科通信技术股份有限公司	5	5
广州竞远安全技术股份有限公司	4	4
福建国科信息科技有限公司-漏斗社区	3	3
内蒙古奥创科技有限公司	2	2
北京信联科汇科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
广州万方计算机科技有限公司	1	1
广州昊达信息科技有限公司	1	1
广州思迈特软件有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	1	1
CNCERT 河北分中心	6	6
CNCERT 广西分中心	3	3
CNCERT 贵州分中心	3	3
CNCERT 江苏分中心	3	3
CNCERT 吉林分中心	1	1

个人	148	148
报送总计	3139	1994

本周漏洞按类型和厂商统计

本周，CNVD 收录了 230 个漏洞。WEB 应用 96 个，应用程序 88 个，操作系统 27 个，数据库 10 个，网络设备（交换机、路由器等网络端设备）7 个，智能设备（物联网终端设备）漏洞 1 个，安全产品 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
WEB 应用	96
应用程序	88
操作系统	27
数据库	10
网络设备（交换机、路由器等网络端设备）	7
智能设备（物联网终端设备）漏洞	1
安全产品	1

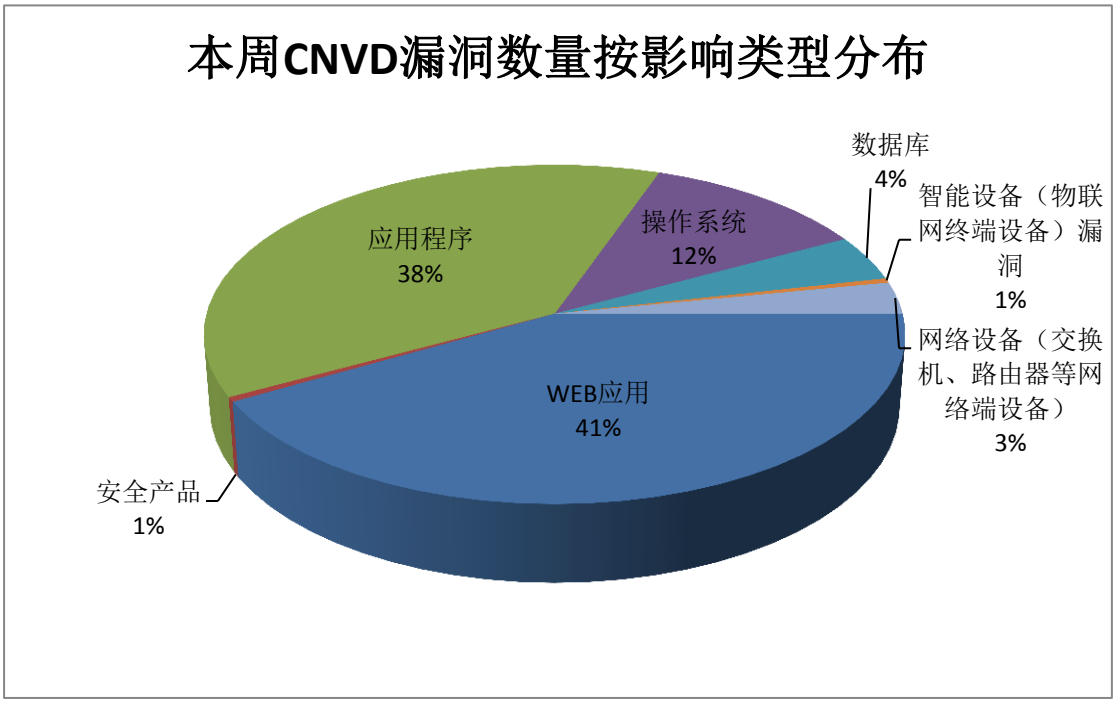

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Joomla!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	18	8%
2	Microsoft	18	8%
3	Joomla!	18	8%
4	Cisco	11	5%
5	Google	10	4%
6	Oracle	10	4%
7	CloudBees	9	4%
8	UltraVNC	8	3%
9	OpenEMR	7	3%
10	其他	121	53%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，19 个移动互联网行业漏洞，7 个工控行业漏洞，（如下图所示）。其中，“Cisco IOS XE 任意文件上传漏洞、Siemens SINEMA 未经授权访问漏洞、Google Android System 远程代码执行漏洞（CNVD-2019-10473）、Cisco IOS XE ETA 拒绝服务漏洞”等漏洞的综合评级为“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/

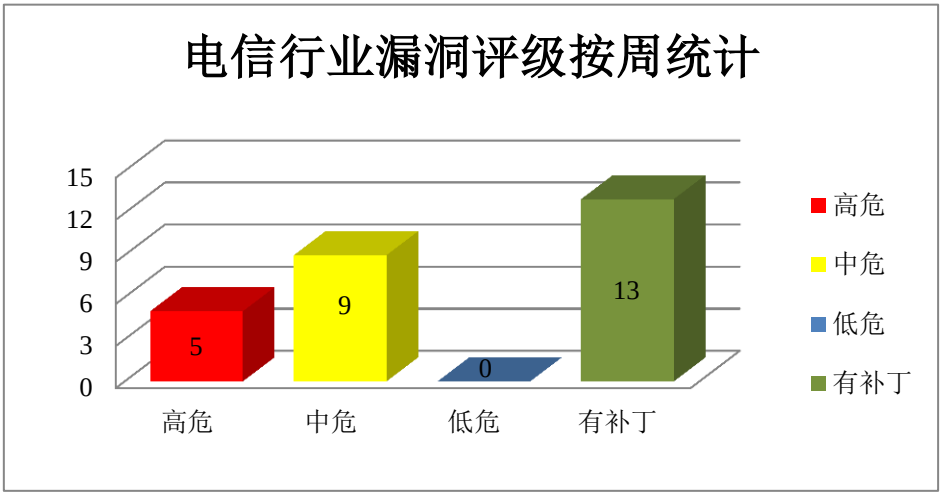

图 3 电信行业漏洞统计

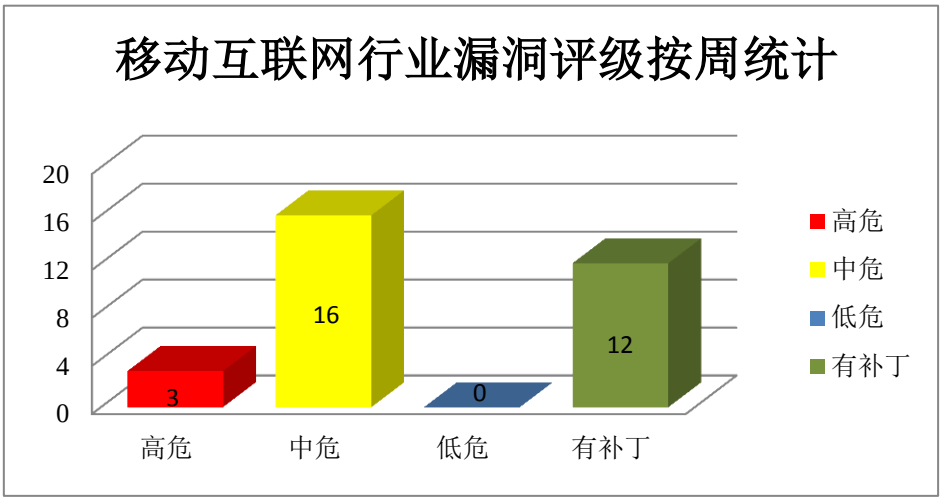

图 4 移动互联网行业漏洞统计

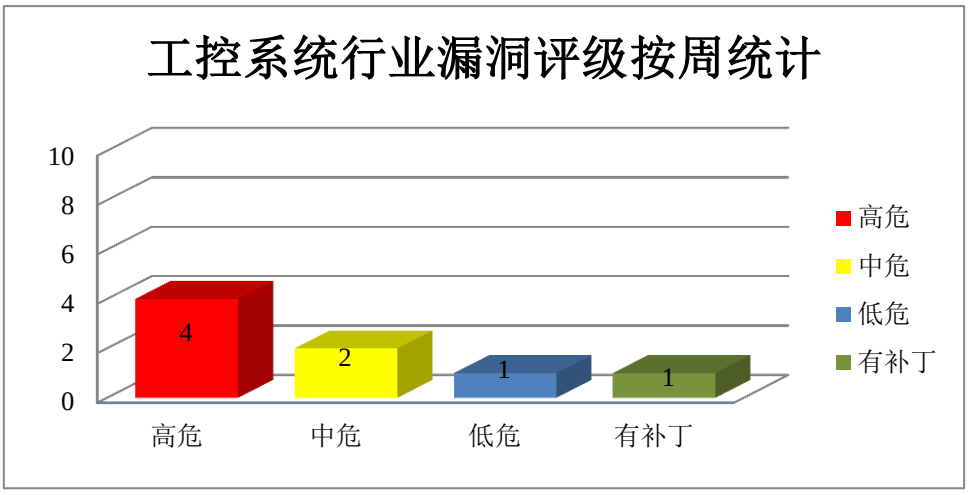

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Bridge 是一款免费数字资产管理应用程序。Adobe Shockwave Player 是一款多媒体播放器产品。本周，上述产品被披露存在内存错误引用和内存破坏漏洞，攻击者可利用漏洞获取信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Bridge CC 内存错误引用漏洞、Adobe Shockwave Player 内存破坏漏洞（CNVD-2019-10620、CNVD-2019-10621、CNVD-2019-10623、CNVD-2019-10622、CNVD-2019-10625、CNVD-2019-10624、CNVD-2019-10626）。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-2019-09858

http://www.cnvd.org.cn/flaw/show/CNVD-2019-10620
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10621
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10623
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10622
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10625
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10624
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10626

2、Microsoft 产品安全漏洞

Windows 是美国微软公司研发的一套操作系统，Windows 采用了图形化模式 GUI。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，造成内存破坏。

CNVD 收录的相关漏洞包括：Microsoft Windows Win32k 权限提升漏洞（CNVD-2019-10041、CNVD-2019-10043、CNVD-2019-10042）、Microsoft Internet Explorer VBScript 引擎远程代码执行漏洞、Microsoft Internet Explorer 脚本引擎内存破坏漏洞（CNVD-2019-10617、CNVD-2019-10616）、Microsoft Internet Explorer VBScript 引擎远程代码执行漏洞（CNVD-2019-10619、CNVD-2019-10618）。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-2019-10041
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10043
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10042
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10615
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10617
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10616
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10619
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10618

3、Cisco 产品安全漏洞

Cisco IOS XE 是一个基于 Linux 内核的模块化操作系统。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，以 root 用户身份执行任意命令或造成拒绝服务。

CNVD 收录的相关漏洞包括：Cisco IOS XE 命令注入漏洞（CNVD-2019-10454、CNVD-2019-10460、CNVD-2019-10462）、Cisco IOS XE 权限提升漏洞（CNVD-2019-10455、CNVD-2019-10463）、Cisco IOS XE ETA 拒绝服务漏洞、Cisco IOS XE 任意文件上传漏洞、Cisco IOS XE 信息泄露漏洞。其中，除“Cisco IOS XE 信息泄露漏洞、

Cisco IOS XE 命令注入漏洞（CNVD-2019-10462）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-10454
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10455
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10458
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10459
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10460
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10461
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10462
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10463

4、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2019-10367、CNVD-2019-10369、CNVD-2019-10368、CNVD-2019-10372、CNVD-2019-10374、CNVD-2019-10373、CNVD-2019-10376、CNVD-2019-10375）。其中，除“Oracle MySQL Server 拒绝服务漏洞（CNVD-2019-10367、CNVD-2019-10369、CNVD-2019-10372）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-10367
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10369
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10368
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10372
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10374
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10373
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10376
http://www.cnvd.org.cn/flaw/show/CNVD-2019-10375

5、D-Link DI-524 跨站脚本漏洞

D-Link DI-524 是一款无线路由器。D-Link DI-524 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。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-10325

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-2019-09849	Adobe Acrobat 和 Reader 越界写入漏洞（CNVD-2019-09849）	高	厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb18-41.html
CNVD-2019-10017	Nagios XI SQL 注入漏洞（CNVD-2019-10017）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.nagios.com/products/security/
CNVD-2019-10132	libcurl 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/curl/curl/commit/57d299a499155d4b327e341c6024e293b0418243.patch
CNVD-2019-10145	OpenEMR SQL 注入漏洞（CNVD-2019-10145）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/openemr/openemr/pull/1758/files
CNVD-2019-10286	UltraVNC 越界访问漏洞（CNVD-2019-10286）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.uvnc.com/
CNVD-2019-10293	UltraVNC 堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.uvnc.com/
CNVD-2019-10448	IBM BigFix Platform 未授权操作漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www-01.ibm.com/support/docview.wss?uid=ibm10874666
CNVD-2019-10457	Forcepoint Email Security 缓冲区溢出漏洞	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.forcepoint.com/KBArticle?id=000016621
CNVD-2019-10464	Google Android 缓冲区溢出漏洞（CNVD-2019-10464）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2019-02-01
CNVD-2019-10628	Adobe Acrobat 和 Reader 内存错误引用漏洞（CNVD-2019-10628）	高	厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb19-17.html

小结：本周，Adobe 被披露存在内存错误引用和内存破坏漏洞，攻击者可利用漏洞

获取信息，执行任意代码。此外，Microsoft、Cisco、Oracle 等多款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，造成内存破坏等。另外，D-Link DI-524 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、Apache Axis 代码执行漏洞

验证描述

Apache Axis 是一个开源、基于 XML 的 Web 服务架构。

Apache Axis 1.4 版本中存在安全漏洞。远程攻击者可利用该漏洞执行代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/46682

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-10449

信息提供者

深信服科技股份有限公司

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. WPA3 标准被曝“超大”WiFi 安全漏洞

两名安全研究人员披露了 Wi-Fi WPA3 标准中的一组漏洞，这组漏洞被命名为 Dragonblood。攻击者可利用这些漏洞在受害者网络范围内获取 Wi-Fi 密码和渗透进网络。Dragonblood 由五个漏洞构成，包括一个拒绝访问攻击，两个降级攻击和两个侧通道信息泄露。后四个漏洞都利用了 WPA3 标准 Dragonfly 密钥交换机制中的设计缺陷，可用于获取用户密码。研究人员发现的攻击方法可玩弄 WPA3 用于验证网络上设备的 Dragonfly 握手系统。利用得当的话，攻击者无需知晓密码即可登入目标网络。具体来说，攻击者可读取 WPA3 本应安全加密的信息，进而盗取信用卡、密码、聊天内容、电子邮件等等敏感信息——如果没有额外采取 HTTPS 之类保护措施的话。

参考链接：https://www.secrss.com/articles/9914

2. 美国天气频道遭勒索软件攻击，停止直播 1 个多小时

根据《华尔街日报》的报道，The Weather Channel 本周四遭遇勒索软件攻击，并暂时停止了一个直播节目的播出。此次攻击发生在美国东南部遭遇恶劣天气袭击之际，

导致这家有线电视频道瘫痪了一个多小时。联邦调查局（FBI）表示，这是一次勒索软件攻击，该部门正在展开调查。The Weather Channel 在 Twitter 上表示：“在网络遭到恶意软件攻击之后，我们今天上午的直播出现了问题。”该频道同时表示，已经通过“备份机制”恢复了服务。“我们为给观众带来的不便表示道歉，我们正在努力解决这个问题。”

参考链接：https://tech.sina.com.cn/i/2019-04-20/doc-ihvhiewr7233865.shtml

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