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 08 日-2019 年 04 月 15 日　　2019 年第 15 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 135 个，其中高危漏洞 47 个、中危漏洞 77 个、低危漏洞 11 个。漏洞平均分值为 6.05。本周收录的漏洞中，涉及 0day 漏洞 40 个（占 30%），其中互联网上出现“libIEC61850 缓冲区溢出漏洞（CNVD-2019-09613）、Hoosk PHP 代码执行漏洞”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 1755 与上周（1599 个）环比增长 10%。

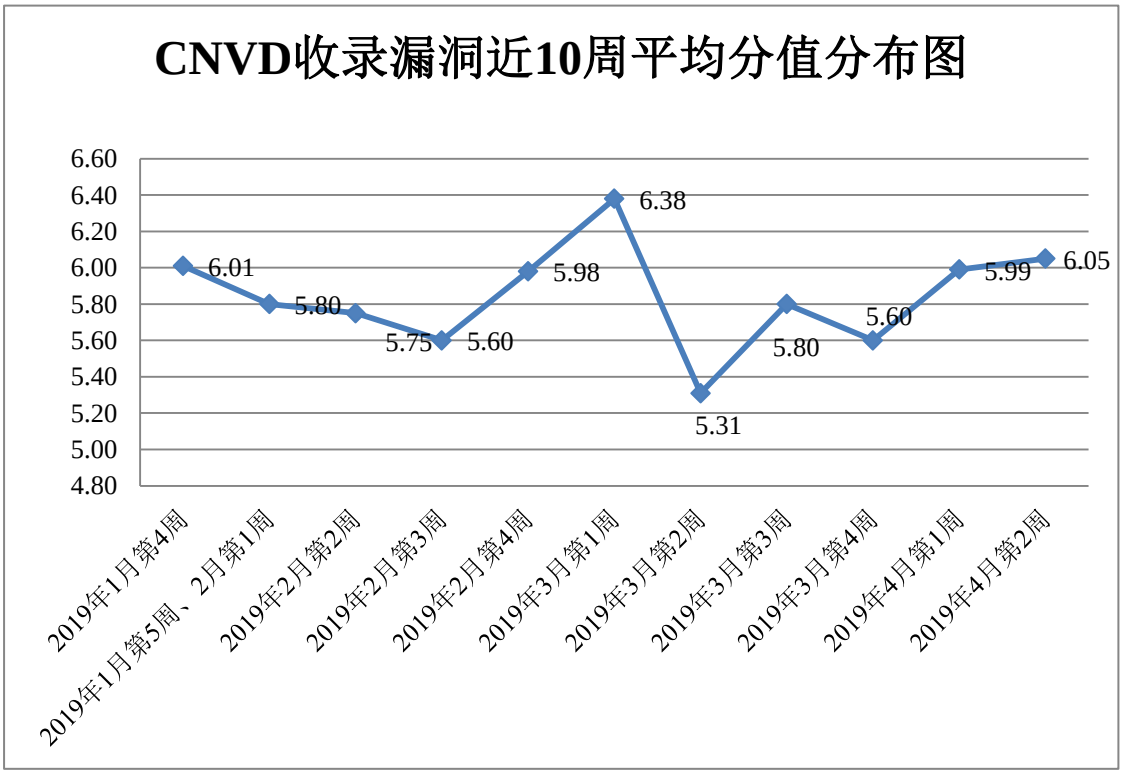

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 起，向银行、保险、能源等重要行业单位通报漏洞事件 4 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 232 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 20 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：

索尼（中国）有限公司、灵吉网络科技有限公司、淄博闪灵网络科技有限公司、广东凯格网络科技有限公司、石家庄民友网络科技有限公司、厦门得推网络科技有限公司、北京希遇信息科技有限公司、西安利友科技有限公司、中铁电气化局集团第一工程有限公司、上海五五来客科技股份有限公司、景腾多媒体股份有限公司、合肥一浪网络科技有限公司、天津市企商科技发展有限公司、三一网络技术有限公司、中交第四航务工程局有限公司、上海茸易科技有限公司、国家焊接材料质量监督检验中心、国家农产品现代物流工程技术研究中心、国家气象信息中心、中国电子商务认证中心、中国建筑防水协会、中国建筑装饰协会施工委员会、中国民办教育协会、环球华讯网、速通物流网、中国村镇发展网、中国 CMA 考试网、如斯团队、海洋 CMS、iCMS、JYmusic、爱客 CMS、超级 cms 和 ForestBlog。

本周，CNVD 发布了《Microsoft 发布 2019 年 4 月安全更新》、《关于 Atlassian Confluence Widget Connector 存在目录穿越、远程代码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/4975

http://www.cnvd.org.cn/webinfo/show/4977

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、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、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。长春嘉诚信息技术股份有限公司、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、天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）、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、山石网科通信技术股份有限公司、北京信联科汇科技有限公司、上海并擎软件科技有限公司、南京联成科技发展股份有限公司、山东华鲁科技发展股份有限公司、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、安徽长泰信息安全服务有限公司、成都安美勤信息技术股份有限公司、江苏通付盾信息安全技术有限公司、广州市眯眼猫信息科技有限公司及其他个人白帽子向 CNVD 提交了 1755 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 1244 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）	750	750
360 网神（补天平台）	494	494
北京天融信网络安全技术有限公司	282	1
哈尔滨安天科技集团股份有限公司	215	0
新华三技术有限公司	202	0
深信服科技股份有限公司	174	0
华为技术有限公司	141	0
北京启明星辰信息安全技术有限公司	41	1
四川无声信息技术有限公司	31	31
北京数字观星科技有限公司	29	0
恒安嘉新(北京)科技股份公司	27	0
中国电信集团系统集成有限责任公司	20	0
北京神州绿盟科技有限公司	19	0
北京知道创宇信息技术有限公司	7	7
长春嘉诚信息技术股份有限公司	106	106
中新网络信息安全股份有限公司	57	57
安徽锋刃信息科技有限公司	48	48
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	46	46
北京圣博润高新技术股份有限公司	28	28

山东云天安全技术有限公司	13	13
山石网科通信技术股份有限公司	4	4
北京信联科汇科技有限公司	4	4
上海并擎软件科技有限公司	4	4
南京联成科技发展股份有限公司	3	3
山东华鲁科技发展股份有限公司	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
安徽长泰信息安全服务有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
江苏通付盾信息安全技术有限公司	1	1
广州市眯眼猫信息科技有限公司	1	1
CNCERT 西藏分中心	2	2
CNCERT 北京分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 吉林分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	141	141
报送总计	2903	1755

本周漏洞按类型和厂商统计

本周，CNVD 收录了 135 个漏洞。应用程序 72 个，操作系统 36 个，WEB 应用 26 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
应用程序	72
操作系统	36
WEB 应用	26
安全产品	1

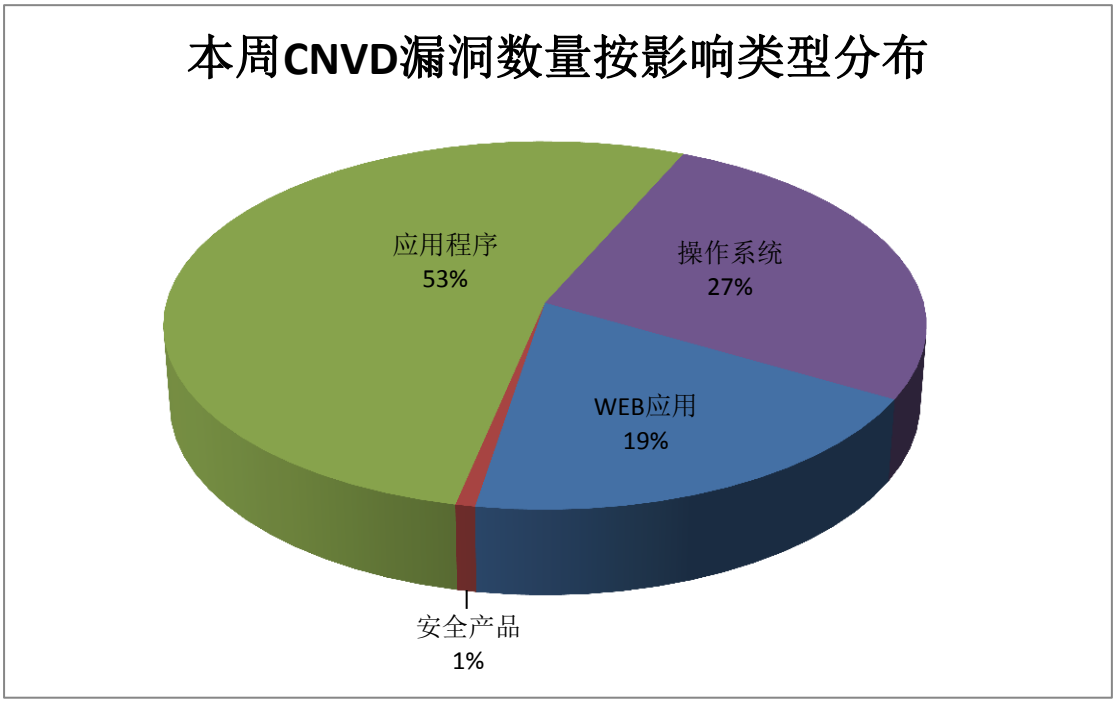

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Microsoft、SAP 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	Apple	26	20%
2	Microsoft	10	7%
3	SAP	10	7%
4	CloudBees	9	7%
5	WAVM	9	7%
6	Adobe	6	4%
7	Contiki-NG	5	4%
8	libIEC61850	3	2%
9	LuPng	3	2%
10	其他	54	40%

本周行业漏洞收录情况

本周，CNVD 收录了 1 个电信行业漏洞，29 个移动互联网行业漏洞，3 个工控行业漏洞，（如下图所示）。其中，“多款 Apple 产品 iAP 和 CoreCrypto 缓冲区溢出漏洞、Apache Tomcat 远程代码执行漏洞（CNVD-2019-09856）、多款 Apple 产品 Power Management 输入验证漏洞、Rockwell Automation RSLinx Classic 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/

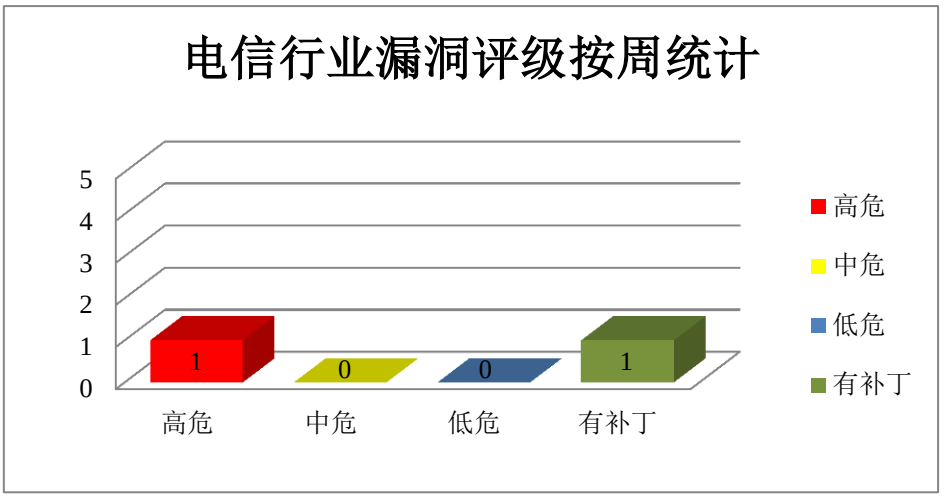

图 3 电信行业漏洞统计

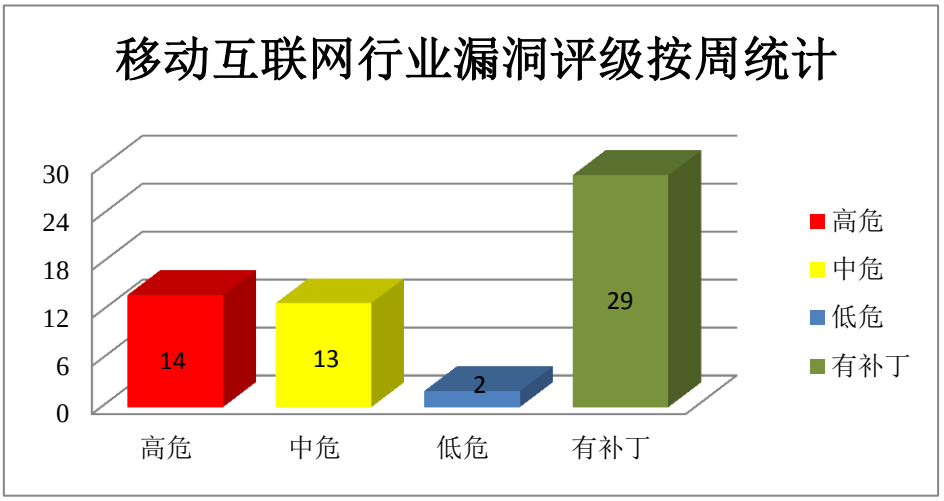

图 4 移动互联网行业漏洞统计

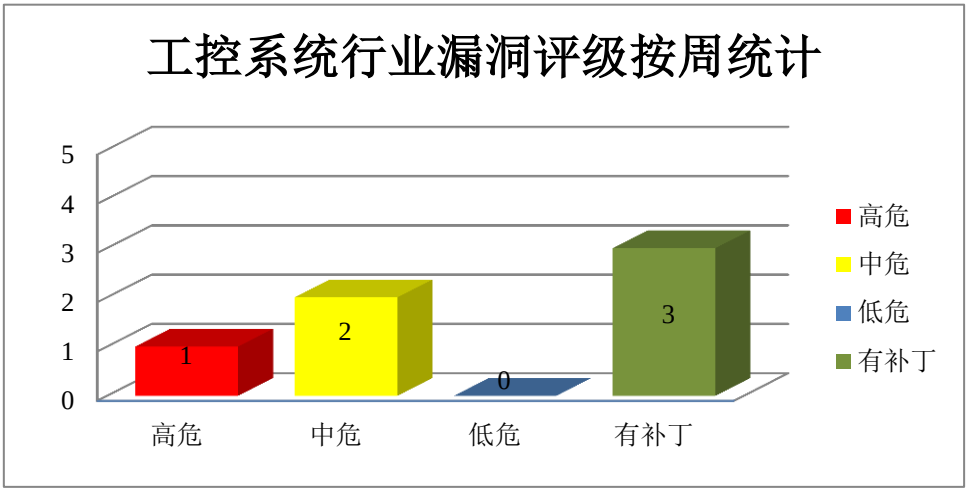

图 5 控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple Safari 是一款 Web 浏览器，是 MacOSX 和 iOS 操作系统附带的默认浏览器。Apple iOS 是为移动设备所开发的一套操作系统。Apple tvOS 是一套智能电视操作系统。本周，上述产品被披露存在权限提升和内存破坏漏洞，攻击者可利用漏洞提升权限、执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：Apple iOS 和 Apple macOS Mojave Contacts 权限提升漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-09740、CNVD-2019-09741、CNVD-2019-09743、CNVD-2019-09746、CNVD-2019-09745、CNVD-2019-09748、CNVD-2019-09747）。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-2019-09734

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09740

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09741

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09743

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09746

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09745

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09748

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09747

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 Jet Database Engine 是一个底层数据库引擎。Azure DevOps Server 原名 Team Foundation Server (TFS)，是本地托管的一组协作式软件开发工具。Azure DevOps Server 与现有 IDE 或编辑器集成，可使跨职能团队有效处理各种规模的项目。Team Foundation Server 是 Microsoft 产品，提供源代码管理、报告、需求管理、项目管理、自动构建、实验室管理、测试及发布管理功能。本周，上述产品被披露存在跨站脚本和远程代码执行漏洞，攻击者可利用漏洞进行跨站脚本攻击，在受害者系统上执行任意代码。

CNVD 收录的相关漏洞包括：Azure DevOps Server 和 Team Foundation Server 跨站脚本漏洞（CNVD-2019-09614、CNVD-2019-09616、CNVD-2019-09615）、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2019-09622、CNVD-2019-09621、CNVD-2019-09623、CNVD-2019-09625、CNVD-2019-09624）。其中，除“Azure DevOps Server 和 Team Foundation Server 跨站脚本漏洞（CNVD-2019-09614、CNVD-2019-09616、CNVD-2019-09615）”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-2019-09614

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09616

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09615

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09622

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09621

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09623

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09625

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09624

3、SAP 产品安全漏洞

SAP NetWeaver 是一个面向服务的应用和集成平台,为 SAP 的应用提供开发和运行环境，也可以用来和其它应用和系统进行自定义的开发和集成。SAP HANA 是一套高性能的实时数据分析平台，它提供数据查询功能，用户可直接对大量实时业务数据进行查询和分析。Extended Application Services（XS）是一个应用服务器、Web 服务器和 SAP HANA System 内 Web 应用的开发环境。SAP BusinessObjects Business Intelligence（BI）Platform Servers 是一套商务智能软件和企业绩效解决方案套件。SAP HCM Fiori People Profile GBX01 HR 是一款人力资源管理解决方案。SAP Mobile Platform（SMP）是一套移动应用开发平台。Offline OData application 是其中的一个离线 OData 服务应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问控制器资源，获取敏感信息，注入任意的 Web 脚本或 HTML 等。

CNVD 收录的相关漏洞包括：SAP NetWeaver Process Integration 信息泄露漏洞、SAP NetWeaver AS JAVA 跨站脚本漏洞（CNVD-2019-09631）、SAP HANA Extended

Application Services 信息泄露漏洞（CNVD-2019-09633）、SAP HANA 拒绝服务漏洞（CNVD-2019-09632）、SAP BusinessObjects BI Platform Servers 信息泄露漏洞、SAP HCM Fiori People Profile GBX01 HR 提权漏洞、SAP Mobile Platform server Offline OData 信息泄露漏洞、SAP NetWeaver Process Integration 信息泄露漏洞（CNVD-2019-09637）。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-2019-09628

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09631

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09633

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09632

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09634

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09635

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09636

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09637

4、CloudBees 产品安全漏洞

CloudBees Jenkins 是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具，它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。本周，该产品被披露存在信息泄露和服务器端请求伪造漏洞，攻击者可利用漏洞获取敏感信息，执行恶意操作。

CNVD 收录的相关漏洞包括：CloudBees Jenkins TraceTronic ECU-TEST Plugin 服务器端请求伪造漏洞、CloudBees Jenkins Maven Artifact ChoiceListProvider (Nexus) Plugin 信息泄露漏洞、CloudBees Jenkins Accurev Plugin 信息泄露漏洞、CloudBees Jenkins Anchore Container Image Scanner Plugin 信息泄露漏洞、CloudBees Jenkins meliora-testlab Plugin 信息泄露漏洞、CloudBees Jenkins Resource Disposer Plugin 跨站请求伪造漏洞、CloudBees Jenkins SSH Agent Plugin 信息泄露漏洞、CloudBees Jenkins Confluence Publisher Plugin 服务器端请求伪造漏洞。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-2019-09840

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09842

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09841

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09844

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09843

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09846

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09845

http://www.cnvd.org.cn/flaw/show/CNVD-2019-09847

5、LuPng 堆缓冲区溢出漏洞

LuPng 是一款 PNG 格式解码/编码器。LuPng 被披露存在堆缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码或造成拒绝服务。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-2019-09764

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-2019-09479	IBM API Connect 提权漏洞（CNVD-2019-09479）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.ibm.com/support/docview.wss?uid=ibm10879575
CNVD-2019-09592	Mini-XML 缓冲区溢出漏洞（CNVD-2019-09592）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/michaelrsweet/mxml/commit/4f5577dd4672d228e4180f06bdbd66f343ea45e0
CNVD-2019-09595	Perl 堆溢出漏洞（CNVD-2019-09595）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://metacpan.org/changes/release/SHAY/perl-5.26.3
CNVD-2019-09730	多款 Apple 产品 WebKit 内存错误引用漏洞（CNVD-2019-09730）	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.apple.com/zh-cn/HT209599
CNVD-2019-09751	多款 Apple 产品 Power Management 输入验证漏洞	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.apple.com/zh-cn/HT209599
CNVD-2019-09765	Rockwell Automation RSLinx Classic 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://rockwellautomation.custhelp.com/app/answers/detail/a_id/1075712
CNVD-2019-09854	Adobe Acrobat 和 Reader 越界写入漏洞（CNVD-2019-09854）	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
CNVD-2019-09856	Apache Tomcat 远程代码执行漏洞（CNVD-2019-09856）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://mail-archives.apache.org/mod_mbox/www-announce/201904.mbox/%3C

			13d878ec-5d49-c348-48d4-25a6c81b9605@apache.org%3E
CNVD-2019-09752	多款 Apple 产品 file 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.apple.com/zh-cn/HT209599
CNVD-2019-09851	Adobe Acrobat 和 Reader 越界写入漏洞（CNVD-2019-09851）	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，Apple 被披露存在权限提升和内存破坏漏洞，攻击者可利用漏洞提升权限、执行任意代码（内存破坏）。此外，Microsoft、SAP、CloudBees 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问控制器资源，获取敏感信息，，执行恶意操作，进行跨站脚本攻击，在受害者系统上执行任意代码等。另外，LuPng 被披露存在堆缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码或造成拒绝服务。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、Hoosk PHP 代码执行漏洞

验证描述

Hoosk 是一套以用户为中心的内容管理系统（CMS）。

Hoosk 1.7.0 存在 PHP 代码执行漏洞，攻击者可通过安装期间提供的 SiteUrl 利用该漏洞执行任意代码。

验证信息

POC 链接：https://github.com/havok89/Hoosk/issues/46

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-09785

信息提供者

华为技术有限公司

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. IE 11 浏览器被爆安全漏洞：可远程窃取本地 PC 文件

近日安全专家在 IE 11 浏览器上发现了全新漏洞，在处理.MHT 已保存页面的时候

能够让黑客窃取 PC 上的文件。更为重要的是.MHT 文件格式的默认处理应用程序是 IE 11 浏览器，因此即使将 Chrome 作为默认网页浏览器这个尚未修复的漏洞依然有效。

目前微软还没有计划解决这个问题，微软反馈称：“我们确定在此产品或服务的未来版本中将考虑修复此问题。目前，我们不会持续更新此问题的修复程序状态，我们已关闭此案例。”据悉该漏洞适用于 Windows 7/8.1/10 系统。在微软正式修复 IE 11 浏览器上的漏洞之前，推荐用户尤其是企业用户尽量减少通过 IE 11 浏览器下载和点击不明文件。

参考链接：https://tech.sina.com.cn/i/2019-04-14/doc-ihvhiqax2464092.shtml

2. 中国蚁剑被曝 XSS 漏洞，可导致远程命令执行

中国蚁剑是一款开源的跨平台网站管理工具，它主要面向于合法授权的渗透测试安全人员以及进行常规操作的网站管理员。4 月 12 日凌晨，有用户在中国蚁剑 GitHub 上提交了 issue，称发现中国蚁剑存在 XSS 漏洞，借此可引起 RCE。据悉，该漏洞是因为在 webshell 远程连接失败时，中国蚁剑会返回错误信息，但因为使用的是 html 解析，导致 xss 漏洞。

参考链接：https://www.freebuf.com/news/200765.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