国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 06 月 24 日-2019 年 06 月 30 日 **2019 年第 26 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 201 个，其中高危漏洞 72 个、中危漏洞 86 个、低危漏洞 43 个。漏洞平均分值为 6.23。本周收录的漏洞中，涉及 0day 漏洞 69 个（占 34%），其中互联网上出现“Creatiwity wityCMS SQL 注入漏洞、Quadbase Systems EspressReport ES 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 2575 个，与上周（1736 个）环比增长 48%。

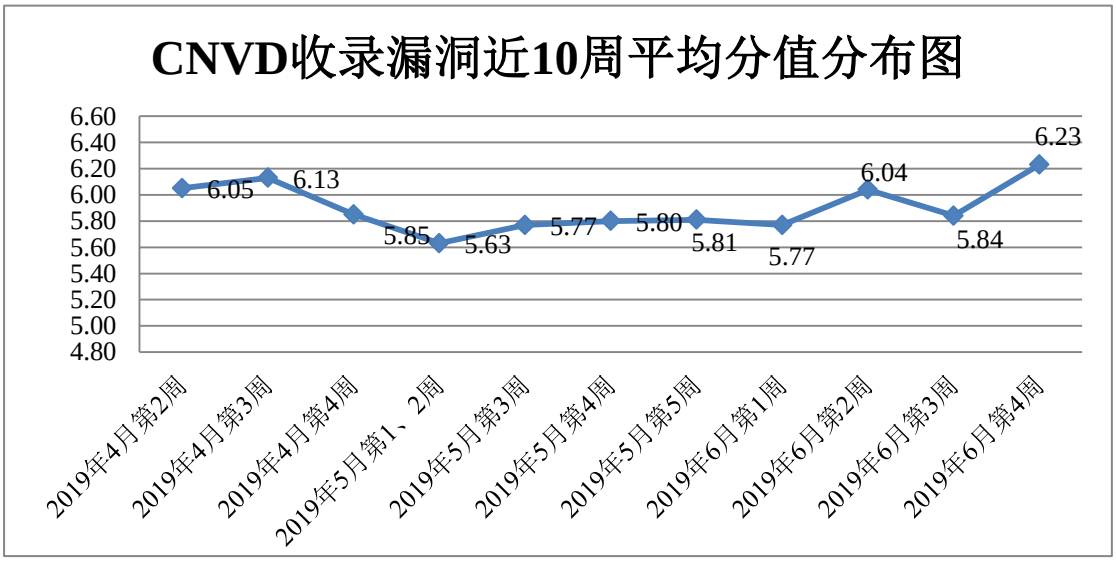

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 34 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 373 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 73 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34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：

上海安达通信息安全技术股份有限公司、研华科技（中国）有限公司、深圳迪元素科技有限公司、广州市佰维网络科技有限公司、北京亚鸿世纪科技发展有限公司、长沙友点软件科技有限公司、杭州海康威视数字技术股份有限公司、成都天睿信息技术有限公司、重庆视动力网络科技有限责任公司、深圳市佳信捷技术股份有限公司、waychar软件公司、江苏国泰新点软件有限公司、厦门才茂通信科技有限公司、北京英富森软件股份有限公司、苏州三三云网络科技有限公司、苏州烟火网络科技有限公司、北京派网软件有限公司、中国社会心理学会、搜狐公司、北京世纪超星信息技术发展有限责任公司、正方软件股份有限公司、智达自动化科技有限公司、友讯科技、广州市互诺计算机科技有限公司、深圳智沃科技有限公司、淄博闪灵网络科技有限公司、中国软件行业协会信息主管（CIO）分会、贝恩斯网络服务中心、waychar、zzzcms、weaveworks、Allok Soft Inc.、Iperius Backup、Tuneclone、Realterm Serial Termianl、Joomla!和 Schneider Electric。

本周，CNVD 发布了《关于 WebSphere 存在远程代码执行漏洞的安全公告》和《关于致远 OA-A8 系统存在远程命令执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5093

https://www.cnvd.org.cn/webinfo/show/5095

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，四川无声信息技术有限公司、中新网络信息安全股份有限公司、南京联成科技发展股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、国网思极检测技术（北京）有限公司、南京众智维信息科技有限公司、内蒙古奥创科技有限公司、长春嘉诚信息技术股份有限公司、山东新潮信息技术有限公司、任子行网络技术股份有限公司、广州锦行网络科技有限公司、上海银基信息安全技术股份有限公司、山东华鲁科技发展股份有限公司、北京铭图天成信息技术有限公司、山东新潮信息技术有限公司、河南信安世纪科技有限公司、福建省海峡信息技术有限公司、北京圣博润高新技术股份有限公司、北京智游网安科技有限公司、广东网安科技有限公司、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、北京冠程科技有限公司、河南金盾信安检测评估中心、山石网科通信技术有限公司及其他个人白帽子向 CNVD 提交了 2575 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1649 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）	1187	1187
奇安信网神（补天平台）	462	462
四川无声信息技术有限公司	43	43
中新网络信息安全股份有限公司	18	18
南京联成科技发展股份有限公司	4	4
北京天融信网络安全技术有限公司	246	2
北京神州绿盟科技有限公司	45	2
北京知道创宇信息技术股份有限公司	1	1
恒安嘉新(北京)科技股份公司	12	1
华为技术有限公司	108	0
哈尔滨安天科技集团股份有限公司	164	0
深信服科技股份有限公司	95	0
新华三技术有限公司	83	0
北京数字观星科技有限公司	20	0
中国电信集团系统集成有限责任公司	6	0
国瑞数码零点实验室	232	232
国网思极检测技术（北京）有限公司	82	82
南京众智维信息科技有限公司	37	37
内蒙古奥创科技有限公司	35	35
长春嘉诚信息技术股份有限公司	33	33
山东新潮信息技术有限公司	26	26

任子行网络技术股份有限公司	25	25
广州锦行网络科技有限公司	12	12
上海银基信息安全技术股份有限公司	11	11
山东华鲁科技发展股份有限公司	9	9
北京铭图天成信息技术有限公司	6	6
山东新潮信息技术有限公司	6	6
河南信安世纪科技有限公司	5	5
福建省海峡信息技术有限公司	4	4
北京圣博润高新技术股份有限公司	3	3
北京智游网安科技有限公司	2	2
广东网安科技有限公司	2	2
上海物盾信息科技有限公司	2	2
浙江鹏信信息科技股份有限公司	2	2
北京冠程科技有限公司	1	1
河南金盾信安检测评估中心	1	1
山石网科通信技术有限公司	1	1
CNCERT 山西分中心	34	34
CNCERT 宁夏分中心	17	17
CNCERT 黑龙江分中心	8	8
CNCERT 甘肃分中心	5	5
CNCERT 四川分中心	5	5
CNCERT 湖南分中心	4	4

CNCERT 西藏分中心	4	4
CNCERT 海南分中心	1	1
个人	240	240
报送总计	3349	2575

本周漏洞按类型和厂商统计

本周，CNVD 收录了 201 个漏洞。应用程序 152 个，WEB 应用 28 个，网络设备（交换机、路由器等网络端设备）13 个，安全产品 6 个，操作系统 1 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	152
WEB 应用	28
网络设备（交换机、路由器等网络端设备）	13
安全产品	6
操作系统	1
智能设备（物联网终端设备）漏洞	1

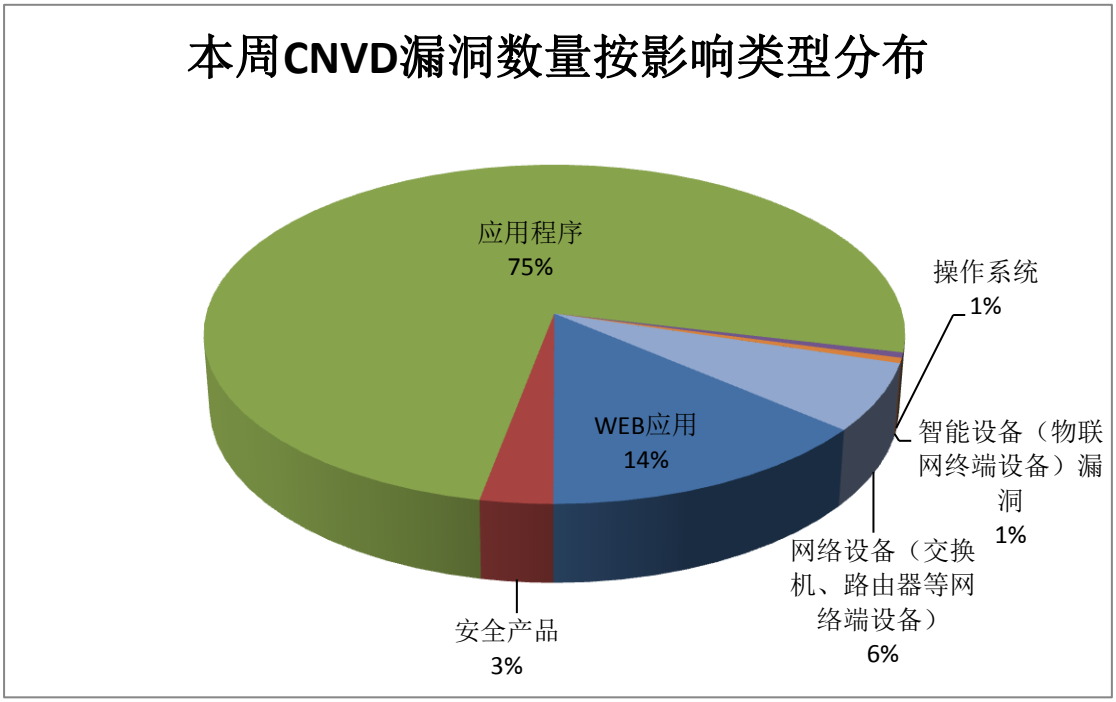

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Cisco、IBM 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	15	8%
2	Cisco	14	7%
3	IBM	13	7%
4	ABB	10	5%
5	PHP Scripts Mall	6	3%
6	Apache	5	2%
7	Michael Elkins	5	2%
8	STOPzilla	5	2%
9	Joomla!	4	2%
10	其他	124	62%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，4 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，“ABB PB610 IDAL HTTP server 缓冲区溢出漏洞、Cisco Data Center Network Manager 认证绕过漏洞、ABB HMI Hardcoded Credentials 文件读取漏洞、Cisco Data Center Network Manager 任意文件上传漏洞”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/

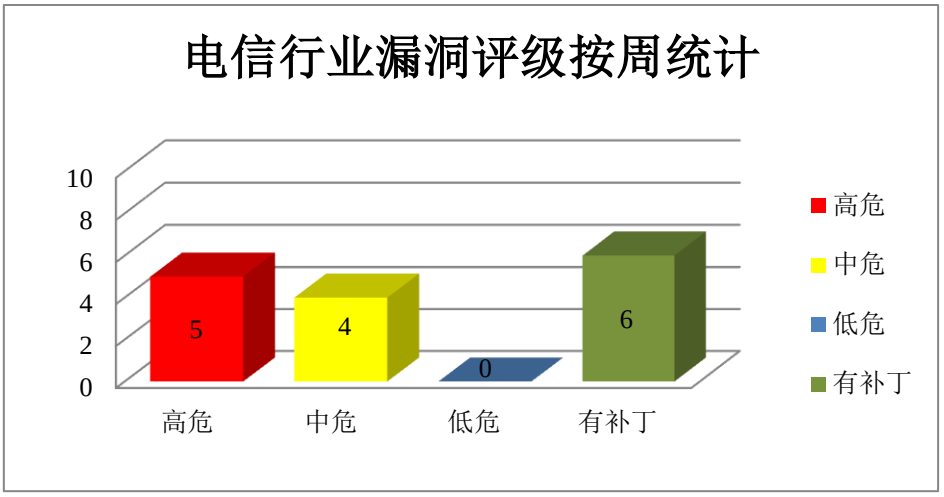

图 3 电信行业漏洞统计

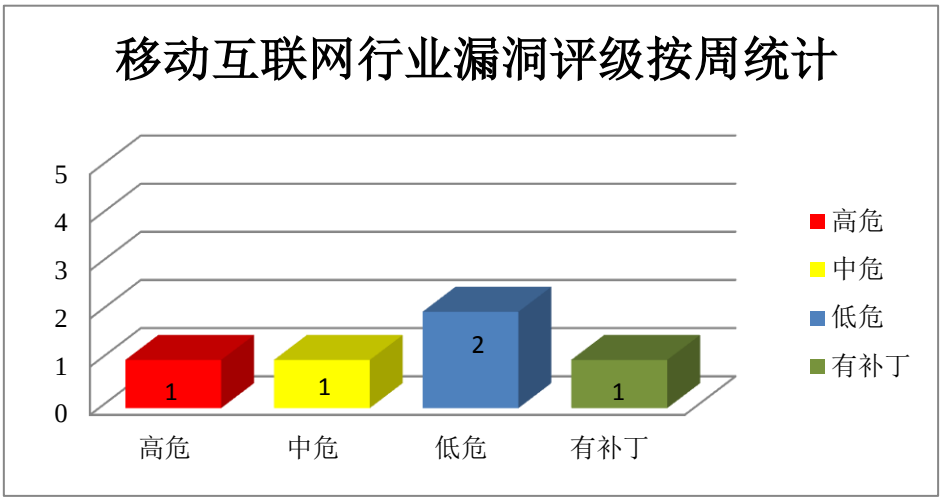

图 4 移动互联网行业漏洞统计

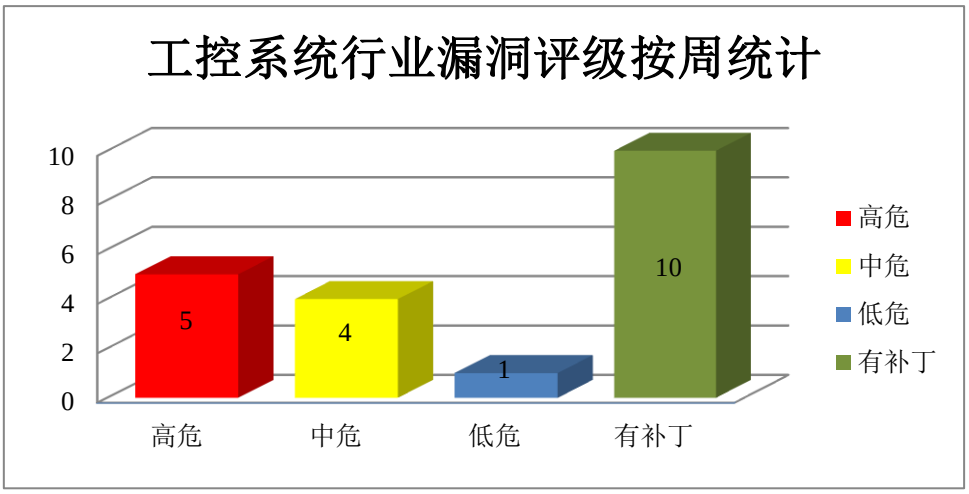

图 5 工控系统行业漏洞统计

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、 WebSphere 存在远程代码执行漏洞

WebSphere Application Server 是一种功能完善、开放的 Web 应用程序服务器，基于 Java 和 Servlets 的 Web 应用程序运行，是 IBM 电子商务计划的核心部分，由于其可靠、灵活和健壮的特点，被广泛应用于企业的 Web 服务中。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞导致任意代码执行。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server ND 远程代码执行漏洞。该漏洞的综合评级为“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-2019-18510

2、致远 OA-A8 系统存在远程命令执行漏洞

致远 OA-A8 是由北京致远互联软件股份有限公司（以下简称致远公司）开发的一款协同管理软件，构建了面向中大型、集团组织的数字化协同运营平台。本周，该产品被披露存在远程命令执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：致远 A8+协同管理软件存在远程命令执行漏洞。该漏洞的综合评级为“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-2019-19299

3、Adobe 产品安全漏洞

Adobe Reader(也被称为 Acrobat Reader)是 Adobe 公司开发的一款 PDF 文件阅读软件。Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。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/Reader 内存错误引用漏洞（CNVD-2019-19836、CNVD-2019-19837、CNVD-2019-19838、CNVD-2019-19839、CNVD-2019-19840、CNVD-2019-19841、CNVD-2019-19842、CNVD-2019-19843）。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-2019-19836
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19837
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19838
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19839
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19840
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19841
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19842
http://www.cnvd.org.cn/flaw/show/CNVD-2019-19843

4、Cisco 产品安全漏洞

Cisco Integrated Management Controller（IMC）是一套用于对 UCS（统一计算系统）进行管理的软件。Cisco SD-WAN Solution 是一套网络扩展解决方案。CLI 是其中的一个命令行界面。Cisco Data Center Network Manager (DCNM)是一套数据中心网络管理器，可对网络进行多协议管理，并对交换机的运行状况和性能提供故障排除功能。Cisco Elastic Services Controller Software（ESC Software）是一套开源的用于管理虚拟资源的模块化系统。本周，该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，执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco Integrated Management Controller 缓冲区溢出漏洞、Cisco Integrated Management Controller 操作系统命令注入漏洞（CNVD-2019-18

899）、Cisco SD-WAN Solution 命令注入漏洞（CNVD-2019-19047）、Cisco Data Center Network Manager 任意文件上传漏洞、Cisco Data Center Network Manager 任意文件下载漏洞、Cisco Elastic Services Controller Software 授权问题漏洞、Cisco Data Center Network Manager 认证绕过漏洞、Cisco Data Center Network Manager 信息泄露漏洞。其中，除“Cisco Integrated Management Controller 缓冲区溢出漏洞、Cisco Data Center Network Manager 信息泄露漏洞”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-2019-18897

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18899

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19047

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19474

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19473

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19823

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19824

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19825

5、IBM 产品安全漏洞

IBM Security Access Manager Appliance（ISAM Appliance）是一款基于网络设备的安全解决方案。IBM License Metric Tool 是一套可帮助 IBM Passport Advantage（软件升级与支持服务）客户决定其处理器价值单元（PVU）许可需求的免费工具。IBM BigFix Inventory 是一套用于软件控制和安全风险缓解的解决方案。IBM Security Information Queue 是美国 IBM 公司的一款数据集成产品。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，注入任意的 JavaScript 代码等。

CNVD 收录的相关漏洞包括：IBM Security Access Manager Appliance 弱加密算法漏洞（CNVD-2019-19294、CNVD-2019-19296）、IBM Security Access Manager Appliance 跨站脚本漏洞、IBM Security Access Manager Appliance 开放重定向漏洞、IBM Security Access Manager Appliance 用户身份验证漏洞、IBM License Metric Tool 和 IBM BigFix Inventory 信息泄露漏洞、IBM Security Information Queue 信息泄露漏洞（CNVD-2019-19829）、IBM Security Information Queue 输入验证错误漏洞。其中，“IBM Security Access Manager Appliance 开放重定向漏洞”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-2019-19294

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19296

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19298

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19297

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19462

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19826

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19829

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19828

6、ABB 产品安全漏洞

ABB PB610 是一款为 CP600 控制面板平台设计图形用户界面的软件。ABB CP635 HMI 是一款人机界面控制面板。ABB CP400PB 是一套人机界面编程软件。CMS-770 是一款用于监测电气系统分支回路的多回路监测系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，获取敏感信息，执行任意代码并造成拒绝服务等。

CNVD 收录的相关漏洞包括：ABB PB610 IDAL HTTP server 缓冲区溢出漏洞、ABB HMI Missing 认证绕过漏洞、ABB PB610 IDAL FTP server 路径遍历漏洞、ABB PB610 IDAL FTP server 格式字符串漏洞、ABB PB610 IDAL HTTP server 身份验证漏洞、ABB HMI Hardcoded Credentials 文件读取漏洞、ABB CMS-770 身份验证绕过漏洞、ABB CP400PB TextEditor 输入验证漏洞。其中，“ABB PB610 IDAL HTTP server 缓冲区溢出漏洞、ABB HMI Missing 认证绕过漏洞、ABB PB610 IDAL FTP server 格式字符串漏洞、ABB HMI Hardcoded Credentials 文件读取漏洞”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-2019-19475

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19478

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19479

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19832

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19830

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19833

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19835

http://www.cnvd.org.cn/flaw/show/CNVD-2019-19834

7、Thompson Reuters UltraTax CS 2017 for Windows 信息泄露漏洞

Thompson Reuters UltraTax CS 2017 for Windows 是一套基于 Windows 平台的自动化税务管理软件。Thompson Reuters UltraTax CS 2017 for Windows 被披露存在信息泄露漏洞。攻击者可利用该漏洞绕过访问控制，获取敏感信息。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-2019-19057

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-2019-19050	Apache Fineract SQL 注入漏洞（CNVD-2019-19050）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cwiki.apache.org/confluence/display/FINERACT/Apache+Fineract+Security+Report
CNVD-2019-19137	Mutt 和 NeoMutt 缓冲区溢出漏洞（CNVD-2019-19137）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gitlab.com/muttmua/mutt/commit/3d9028fec8f4d08db2251096307c0bbbebce669a
CNVD-2019-19206	Juniper Contrail Service Orchestration 未授权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10872&actp=METADATA
CNVD-2019-19284	RDK CcspWifiAgent 模块命令执行漏洞	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://rdkcentral.com/
CNVD-2019-19289	Mozilla Firefox 和 Firefox ESR 安全绕过漏洞（CNVD-2019-19289）	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.mozilla.org/en-US/security/advisories/mfsa2019-19/
CNVD-2019-19302	Atlassian Sourcetree 参数注入漏洞（CNVD-2019-19302）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/SRCTREEWIN-11917
CNVD-2019-19303	Linux kernel 堆缓冲区溢出漏洞（CNVD-2019-19303）	高	厂商已发布漏洞修复程序，请及时关注更新：https://lore.kernel.org/linux-wireless/20190531131841.7552-1-tiwai@suse.de/
CNVD-2019-19309	Adobe ColdFusion 不可信数据反序列化漏洞	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/coldfusion/apsb19-27.html
CNVD-2019-19463	IBM Security Access Manager Appliance 用户冒充漏洞	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-01.ibm.com/support/docview.wss?uid=ibm10888379
CNVD-2019-19471	TP-Link Wi-Fi 扩展器远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://securityaffairs.co/wordpress/872

			63/iot/zero-day-tp-link-wi-fi-extenders.html

小结：本周，WebSphere 被披露存在远程代码执行漏洞，攻击者可利用漏洞导致任意代码执行。致远 OA-A8 系统存在远程命令执行漏洞，攻击者可利用漏洞执行任意代码。此外，Adobe、Cisco、IBM、ABB 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，提升权限，执行任意代码并造成拒绝服务等。Thompson Reuters UltraTax CS 2017 for Windows 被披露存在信息泄露漏洞。攻击者可利用该漏洞绕过访问控制，获取敏感信息。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、Creatiwity wityCMS SQL 注入漏洞

验证描述

Creatiwity wityCMS 是一套基于 PHP 的轻量级内容管理系统（CMS）。

Creatiwity wityCMS 0.6.2 版本中存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令。

验证信息

POC 链接：https://github.com/Creatiwity/wityCMS/issues/157

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-19282

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. Excel 曝出 Power Query 安全漏洞，1.2 亿用户易受远程 DDE 攻击

近日，安全研究人员，发现了微软 Excel 电子表格应用程序的一个新漏洞，或致 1.2 亿用户易受网络攻击。其指出，该安全漏洞意味着攻击者可以利用 Excel 的 Power Query 查询工具，在电子表格上启用远程动态数据交换（DDE），并控制有效负载。此外，Power Query 还能够用于将恶意代码嵌入数据源并进行传播。Mimecast 表示，Power Query 提供了成熟而强大的功能，且可用于执行通常难以被检测到的攻击类型。

参考链接：https://www.cnbeta.com/articles/tech/861981.htm

2. Locked 勒索病毒出山，大肆攻击国内企业

近日，某安全大脑监测到一个使用 Go 语言编写的勒索病毒正在攻击国内企业。该勒索病毒会通过“永恒之蓝”漏洞传播自身，同时加密计算机中的重要文件，将文件后缀修改为“.locked”，之后向受害用户索要赎金 0.2BTC，我们根据其加密后缀将其称为“locked”勒索病毒。

参考链接：https://www.freebuf.com/articles/network/206961.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