国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 03 月 11 日-2019 年 03 月 17 日　　2019 年第 11 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 350 个，其中高危漏洞 70 个、中危漏洞 248 个、低危漏洞 32 个。漏洞平均分值为 5.31。本周收录的漏洞中，涉及 0day 漏洞 131 个（占 37%），其中互联网上出现“XiaoCms 文件上传漏洞、FUEL CMS 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 1675 个，与上周（1916 个）环比下降 13%。

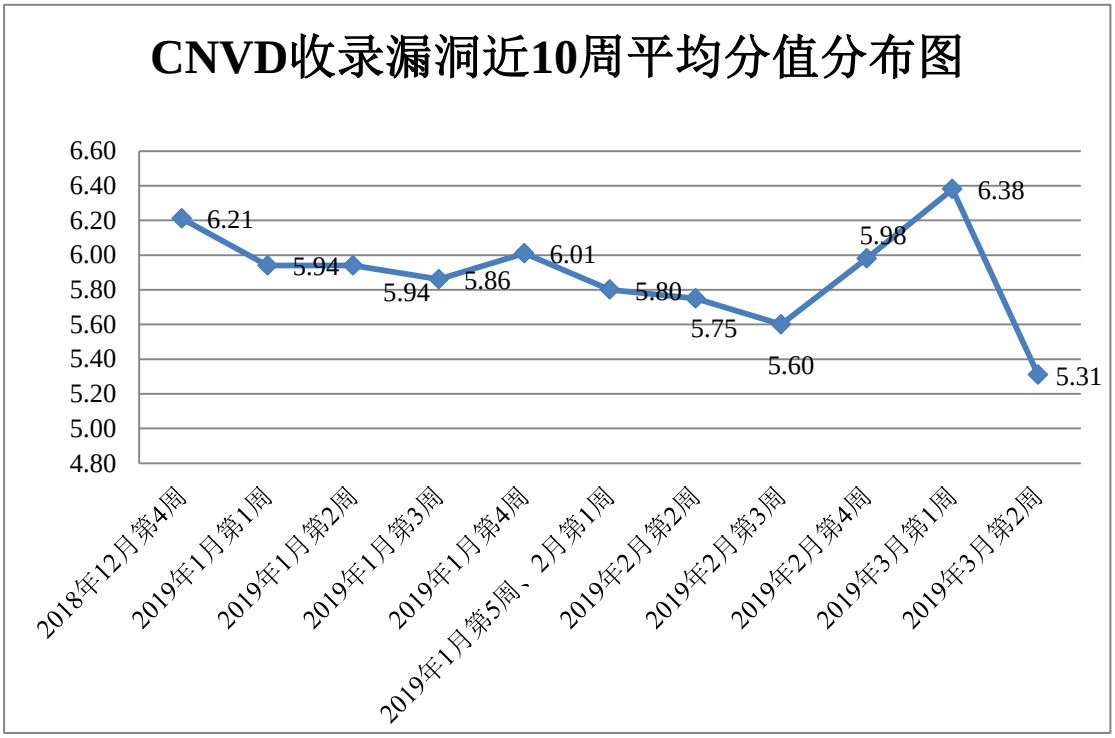

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 起，向银行、保险、能源等重要行

业单位通报漏洞事件 41 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 385 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 39 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 38 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：

长沙米拓信息技术有限公司、上海七慧网络科技有限公司、北京爱奇艺科技有限公司、广州酷狗计算机科技有限公司、济南爱程网络科技有限公司、上海新朋程数据科技发展有限公司、上海卓卓网络科技有限公司、小米科技有限责任公司、枣庄市英特信息网络有限公司、金山软件股份有限公司、太原迅易科技有限公司、好生意 CMS-深圳网站建设公司、广州浩洋信息科技有限公司、成都康菲顿特网络科技有限公司、广州浩洋信息科技有限公司、成都康菲顿特网络科技有限公司、天津恩众科技发展有限公司、苏州托普斯网络科技有限公司、北京城市联盟科技有限公司、武汉贝云网络科技有限公司、西安新软信息科技有限公司、微软(中国)有限公司、北京昌平广播电视网、米酷资源网、八哥软件、互诺科技、爱客 CMS、极点 CMS、里程密 PHP 博客系统、聚擎 cms、Semcms、Vmcms、EARCLINK、Selteco、baigo Studio、Viscom Softwares。

本周，CNVD 发布了《Microsoft 发布 2019 年 3 月安全更新》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4933

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、华为技术有限公司、新华三技术有限公司、北京启明星辰信息安全技术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、任子行网络技术股份有限公司、山东华鲁科技发展股份有限公司、北京圣博润高新技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京国舜科技股份有限公司、内蒙古奥创科技有限公司、山石网科通信技术股份有限公司、北京安信天行科技有限公司、广州竞远安全技术股份有限公司、四川月安客信息技术有限公司、成都安美勤信息技术股份有限公司、华信咨询设计研究院有限公司、南京联成科技发展股份有限公司、山东云天安全技术有限公司、广州万方计算机科技有限公司、山东九州信泰信息科技股份有限公司、中新网络信息安全股份有限公司及其他个人白帽子向 CNVD 提交了 1675 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 1252 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）	776	776
360 网神（补天平台）	476	476
北京天融信网络安全技术有限公司	261	6
哈尔滨安天科技集团股份有限公司	174	0
华为技术有限公司	162	0
新华三技术有限公司	138	0
北京启明星辰信息安全技术有限公司	58	10
北京数字观星科技有限公司	48	0
四川无声信息技术有限公司	45	45
中国电信集团系统集成有限责任公司	38	1
厦门服云信息科技有限公司	25	0
恒安嘉新(北京)科技股份公司	14	0
北京神州绿盟科技有限公司	13	0
深信服科技股份有限公司	9	0
北京知道创宇信息技术有限公司	10	5
沈阳东软系统集成工程有限公司	1	1
国瑞数码零点实验室	84	84
任子行网络技术股份有限公司	20	20
山东华鲁科技发展股份有限公司	11	11
北京圣博润高新技术股份有限公司	9	9
远江盛邦（北京）网络安全科技股份有限公司	8	8

北京国舜科技股份有限公司	6	6
内蒙古奥创科技有限公司	5	5
山石网科通信技术股份有限公司	3	3
北京安信天行科技有限公司	3	3
广州竞远安全技术股份有限公司	3	3
四川月安客信息技术有限公司	3	3
成都安美勤信息技术股份有限公司	2	2
华信咨询设计研究院有限公司	2	2
南京联成科技发展股份有限公司	2	2
山东云天安全技术有限公司	2	2
广州万方计算机科技有限公司	1	1
山东九州信泰信息科技股份有限公司	1	1
中新网络信息安全股份有限公司	1	1
CNCERT 吉林分中心	5	5
CNCERT 广西分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 海南分中心	1	1
CNCERT 宁夏分中心	1	1
个人	180	180
报送总计	2603	1675

本周漏洞按类型和厂商统计

本周，CNVD 收录了 350 个漏洞。应用程序漏洞 202 个，WEB 应用漏洞 63 个，网

络设备漏洞 33 个，数据库漏洞 25 个，操作系统漏洞 20 个，安全产品漏洞 7 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	202
WEB 应用漏洞	63
网络设备漏洞	33
数据库漏洞	25
操作系统漏洞	20
安全产品漏洞	7

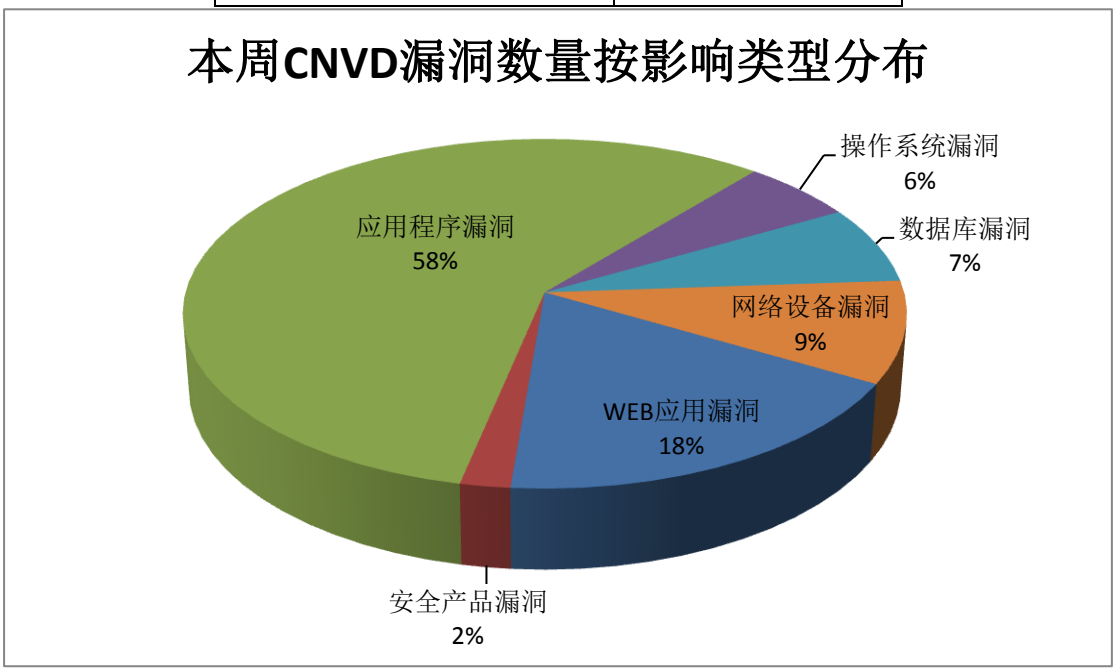

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Infovista、Adobe 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	IBM	33	9%
2	Infovista	24	7%
3	Adobe	23	7%
4	Mcafee	20	6%
5	Oracle	19	5%
6	Microsoft	19	5%
7	TP-LINK	18	5%
8	Google	10	3%

9	Exiv2	8	2%
10	其他	177	51%

本周行业漏洞收录情况

本周，CNVD 收录了 45 个电信行业漏洞，8 个移动互联网行业漏洞，2 个工控行业漏洞，（如下图所示）。其中，“IBM DB2 缓冲区溢出漏洞（CNVD-2019-07259）、Martem TELEM GW6/GWM 提权漏洞、IBM DB2 权限提升漏洞（CNVD-2019-07257）”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/

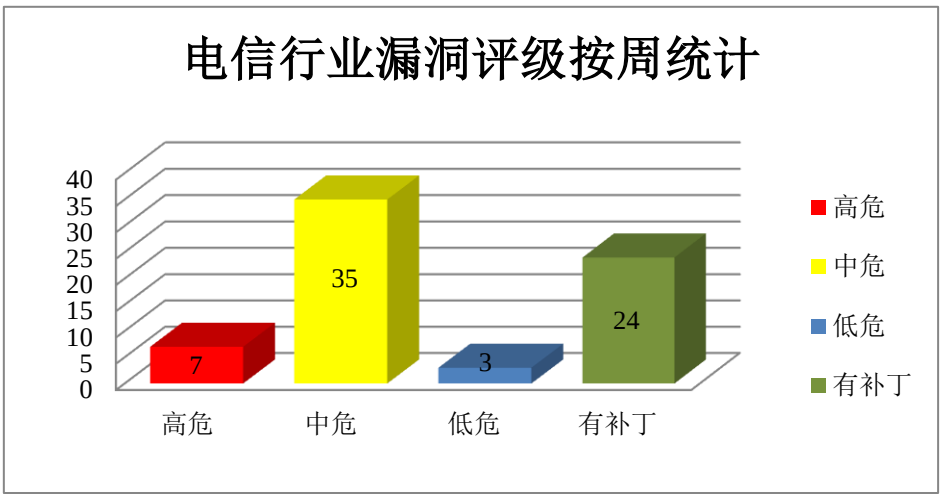

图 3 电信行业漏洞统计

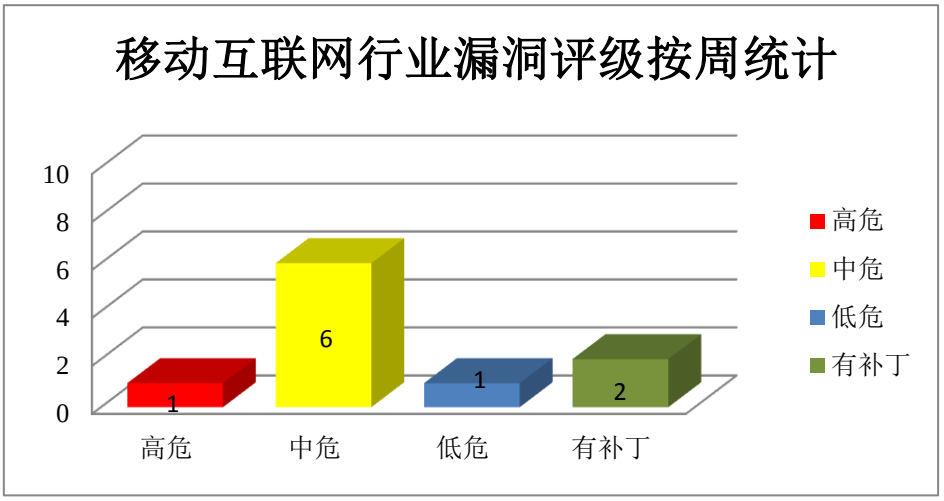

图 4 移动互联网行业漏洞统计

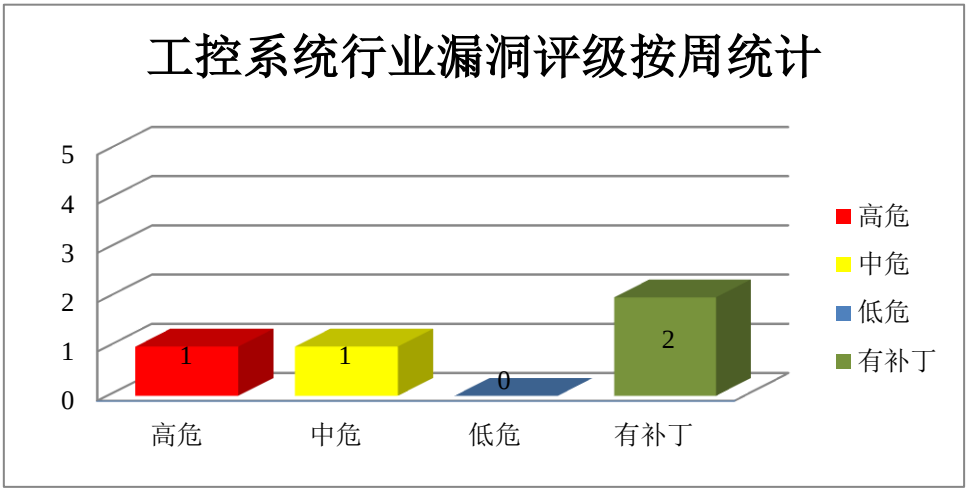

图 5 工控系统行业漏洞统计

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 Acrobat 是一套 PDF 文件编辑和转换工具，Adobe Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在内存错误引用洞，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 内存错误引用洞（CNVD-2019-06905、CNVD-2019-06906、CNVD-2019-06907、CNVD-2019-06908、CNVD-2019-06909、CNVD-2019-06910、CNVD-2019-06911、CNVD-2019-06912）。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-2019-06905

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06906

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06907

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06908

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06909

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06910

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06911

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06912

2、Microsoft 产品安全漏洞

Microsoft Word 是 Office 套件中的一款文字处理软件。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 AppX Deployment Server 是其中的一个应用程序部署服务器。Windows VBScript engine 是其中的一个 VBScript（脚本语言）引擎。Microsoft Edge 是一款 Web 浏览器。C

hakraCore 是使用在其中的一个开源的 Chakra JavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。 Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。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，欺骗，绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Microsoft Word 远程执行代码漏洞、Microsoft Windows VBScript Engine 远程执行代码漏洞、Microsoft ChakraCore 和 Edge 远程内存破坏漏洞、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2019-07239）、Microsoft Edge 远程内存破坏漏洞（CNVD-2019-07242）、Microsoft Windows AppX Deployment Server 本地权限提升漏洞、Microsoft Edge 和 Internet Explorer 远程内存破坏漏洞（CNVD-2019-07329）、Microsoft Visual Studio 远程代码执行漏洞（CNVD-2019-07333）。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-2019-06915
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07197
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07237
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07239
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07242
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07328
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07329
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07333

3、Oracle 产品安全漏洞

Oracle MySQL 是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，上述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（组件挂起或频繁崩溃），影响数据的可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 组件拒绝服务漏洞（CNVD-2019-07339、CNVD-2019-07341、CNVD-2019-07340、CNVD-2019-07342、CNVD-2019-07344、CNVD-2019-07343、CNVD-2019-07346、CNVD-2019-07348）。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-2019-07339
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07341
http://www.cnvd.org.cn/flaw/show/CNVD-2019-07340

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07342

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07344

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07343

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07346

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07348

4、Mcafee 产品安全漏洞

McAfee ePolicy Orchestrator 是一款可扩展的平台,可对安全策略进行集中式策略管理与强制实施。McAfee Total Protection 是一套杀毒软件。McAfee Web Gateway（MWG）是一款安全网关产品。McAfee Agent（MA）是一套提供了 ePolicy Orchestrator（杀毒软件管理平台）与被管理产品之间的安全通信的客户端组件。agent 是其中的一个代理程序。McAfee Application Control 是一套程序管控软件，可阻止设备运行未经授权的应用程序。McAfee Change Control 是一套变更管控软件，可拦截对应用程序的未授权变更。McAfee True Key（TK）是美国迈克菲（McAfee）公司的一款身份验证应用程序。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感数据，绕过产品自我保护机制，篡改策略及产品文件，卸载 McAfee 软件，执行任意命令，造成拒绝服务等。

CNVD 收录的相关漏洞包括：McAfee Agent 提权漏洞、McAfee ePolicy Orchestrator 跨站请求伪造漏洞、McAfee Total Protection (MTP)安全限制绕过漏洞、McAfee Web Gateway 不当输入验证漏洞、McAfee Agent 本地拒绝服务漏洞、McAfee Application Control 和 Change Control 安全限制绕过漏洞、McAfee Agent 临时文件不安全处理漏洞、McAfee True Key 跨站脚本漏洞。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-2019-07153

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07306

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07307

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07310

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07313

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07312

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07314

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07319

5、ASUS GT-AC5300 拒绝服务漏洞

ASUS GT-AC5300 是一款无线路由器。本周，ASUS GT-AC5300 被披露存在拒绝服务漏洞。攻击者可通过发送‘GET / HTTP/1.1\r\n’利用该漏洞造成拒绝服务。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-2019-07077

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-2019-06902	PHP 拒绝服务漏洞（CNVD-2019-06902）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/php/php-src/pull/3672/commits/77f24e6e2c2358ecbedcf8657be7b02a788e8137
CNVD-2019-06918	CMS Made Simple SQL 注入漏洞（CNVD-2019-06918）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://forum.cmsmadesimple.org/viewtopic.php?f=1&t=80285
CNVD-2019-07014	GNU C Library 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://sourceware.org/git/gitweb.cgi?p=glibc.git;a=commit;h=583dd860d5b833037175247230a328f0050dbfe9
CNVD-2019-07031	Martem TELEM GW6/GWM 提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ics-cert.us-cert.gov/advisories/ICSA-18-142-01
CNVD-2019-07073	FUEL CMS SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/daylightstudio/FUEL-CMS/commit/3ce6b558aa18410ebccf376b849898385302c4d8
CNVD-2019-07199	Microsoft Windows RemoteFX 虚拟 GPU 微型端口驱动程序本地权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8471
CNVD-2019-07201	phpMyFAQ CSV 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.phpmyfaq.de/security/advisory-2018-09-02
CNVD-2019-07248	PoDoFo 缓冲区溢出漏洞（CNVD-2019-07248）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/podofo/code/1969
CNVD-2019-07254	IBM DB2 缓冲区溢出漏洞（CNVD-2019-07254）	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=ibm10740413
CNVD-2019-07371	Google Android Kernel 组件权限提升漏洞（CNVD-2019-07371）	高	厂商已发布漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2019-02-01

小结：本周，Adobe 被披露存在内存错误引用洞，攻击者可利用漏洞执行任意代码。此外，Microsoft、Oracle、Mcafee 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，欺骗，绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。另外，ASUS GT-AC5300 被披露存在拒绝服务漏洞。攻击者可通过发送‘GET / HTTP/1.1\r\n’利用该漏洞造成拒绝服务。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、FUEL CMS 跨站请求伪造漏洞

验证描述

FUEL CMS 是一款基于 CodeIgniter 的内容管理系统。

FUEL CMS 1.4 中的 my_profile/edit?inline=存在跨站请求伪造漏洞，远程攻击者可利用该漏洞更改管理员密码。

验证信息

POC 链接：http://www.iwantacve.cn/index.php/archives/48/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-07074

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. WordPress 5.1.1 修复可导致网站被接管的 XSS 漏洞

WordPress 团队修复了 5.1 版本中引入的软件缺陷，该漏洞可能允许潜在的攻击者在启用了评论模块的 WordPress 网站上填写包含恶意代码的评论，来引诱登录管理员访问包含 XSS 有效负载的恶意网站来使用跨站点请求伪造（CSRF）漏洞来接管网站。通过该漏洞在隐藏的 iFrame 的帮助下加载并执行 XSS 有效负载，允许未经身份验证的攻

击者执行任意 HTML 和脚本代码，从而可能接管受攻击的易受攻击的 WordPress 网站。某科技公司表示，“CSRF 漏洞利用了多个逻辑缺陷和错误，组合利用这些错误可导致远程执行代码和完全接管网站”。

参考链接：https://www.bleepingcomputer.com/news/security/wordpress-511-fixes-xss-vulnerability-leading-to-website-takeovers/

2. 海淘需谨慎！户外运动品牌 Kathmandu 网上商店遭黑客攻击

据外媒报道，在澳洲证券交易所上市的全球户外服饰和设备零售商 Kathmandu 披露，该公司在节后销售旺季遭遇数据泄露，客户的个人和支付信息被窃取。Kathmandu 在 Magento 电子商务平台上运营网上商店，过去几年，也曾有犯罪分子在未打补丁的服务器上攻击这个平台，并植入盗卡恶意软件。

参考链接：https://www.easyaq.com/news/1930850210.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