国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 12 月 24 日-2018 年 12 月 30 日 **2018 年第 52 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 414 个，其中高危漏洞 166 个、中危漏洞 219 个、低危漏洞 29 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 245 个（占 59%），其中互联网上出现“WordPress 插件 AutoSuggest 'wpas_keys' SQL 注入漏洞、libxls 拒绝服务漏洞”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 1657 个，与上周（1991 个）环比下降 17%。

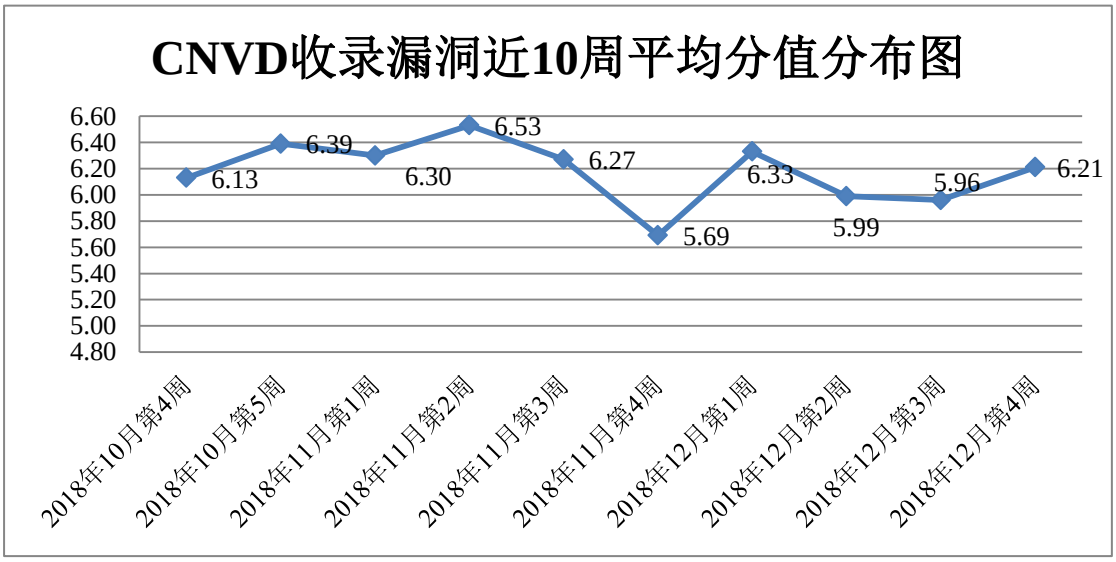

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 起，向银行、保险、能源等重要行业单位通报漏洞事件 44 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 519 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 117 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24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：

上海海天信息系统工程有限公司、用友网络科技股份有限公司、灵宝简好网络科技有限公司、广州得扬网络科技有限公司、淄博闪灵网络科技有限公司、北京若深科技有限公司、北京易维云数据科技有限公司、北京百容千域软件技术开发有限责任公司、湖南翱云网络科技有限公司、南京第五十五所技术开发有限公司、阜阳市心品网络科技有限公司、济南爱程网络科技有限公司、长沙德尚网络科技有限公司、深圳市吉祥腾达科技有限公司、济南点创网络科技有限公司、武汉达梦数据库有限公司、中国电子科技集团公司第五十五研究所、互诺科技、春杰工作室、乐外资源分享网、深圳好生意网络工作室、南充鸿达网络、大河网、和利时集团、安徽启明星工作室、棠下互联、ZZZCMS、HisiPHP、PHPMyWind、Faad2、ZZCMS、TPTCMS、老班 CMS、易贝 CMS。

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、中国电信集团系统集成有限责任公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、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、任子行网络技术股份有限公司、成都思维世纪科技有限公司、河南信安世纪科技有限公司、天津市国瑞数码安全系统股份有限公司、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、南京联成科技发展股份有限公司、上海银基信息安全技术股份有限公司、北京安华金和科技有限公司、江苏百达智慧网络科技有限公司（含光实验室）、吉林省一秋科技有限公司、上海零盾网络科技有限公司、四川月安客信息技术有限公司及其他个人白帽子向 CNVD 提交了 1657 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 1239 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
360 网神（补天平台）	644	644
斗象科技（漏洞盒子）	595	595
北京天融信网络安全技术有限公司	283	22
哈尔滨安天科技集团股份有限公司	265	0

华为技术有限公司	248	6
新华三技术有限公司	116	0
中国电信集团系统集成有限责任公司	62	3
北京神州绿盟科技有限公司	51	0
北京数字观星科技有限公司	47	0
恒安嘉新(北京)科技股份公司	37	0
深信服科技股份有限公司	10	0
北京知道创宇信息技术有限公司	5	0
沈阳东软系统集成工程有限公司	2	2
杭州安恒信息技术股份有限公司	1	1
山东云天安全技术有限公司	43	43
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	24	24
北京圣博润高新技术股份有限公司	21	21
任子行网络技术股份有限公司	10	10
成都思维世纪科技有限公司	9	9
河南信安世纪科技有限公司	9	9
天津市国瑞数码安全系统股份有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京国舜科技股份有限公司	2	2
南京联成科技发展股份有限公司	2	2
上海银基信息安全技术股份有限公司	2	2

北京安华金和科技有限公司	1	1
江苏百达智慧网络科技有限公司（含光实验室）	1	1
吉林省一秋科技有限公司	1	1
上海零盾网络科技有限公司	1	1
四川月安客信息技术有限公司	1	1
CNCERT 吉林分中心	13	13
CNCERT 宁夏分中心	6	6
CNCERT 四川分中心	5	5
CNCERT 北京分中心	4	4
CNCERT 山西分中心	4	4
CNCERT 湖南分中心	3	3
CNCERT 西藏分中心	3	3
CNCERT 上海分中心	1	1
个人	171	171
报送总计	2750	1657

本周漏洞按类型和厂商统计

本周，CNVD 收录了 414 个漏洞。应用程序漏洞 201 个，WEB 应用漏洞 131 个，操作系统漏洞 58 个，网络设备漏洞 18，安全产品漏洞 6 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	201
WEB 应用漏洞	131
操作系统漏洞	58
网络设备漏洞	18
安全产品漏洞	6

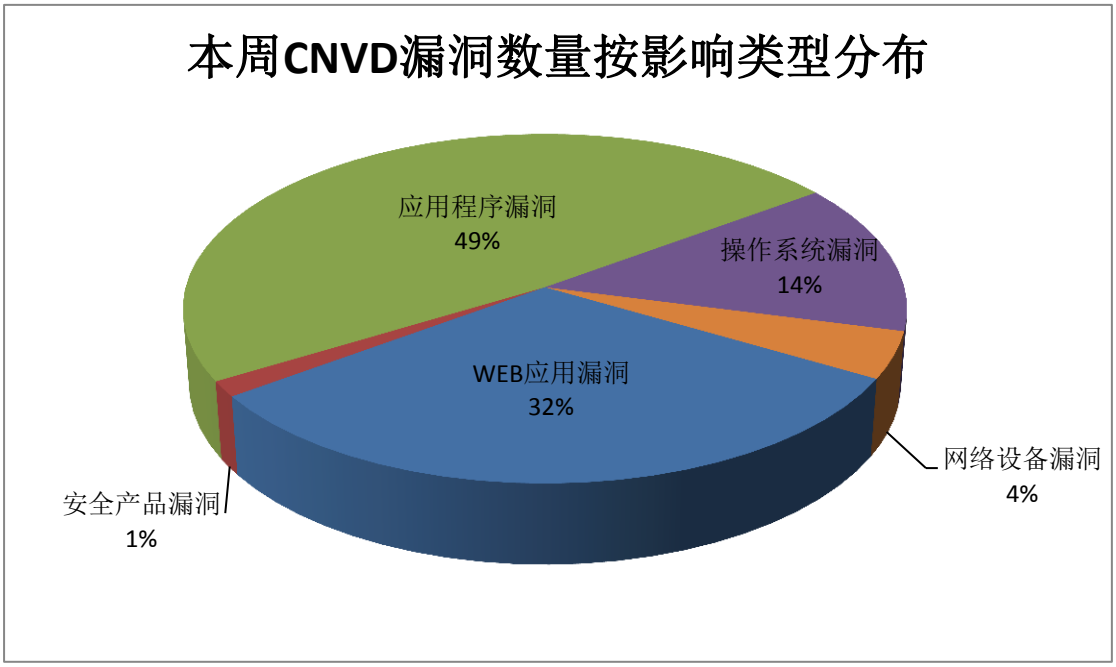

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、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	34	8%
2	Microsoft	24	6%
3	IBM	23	6%
4	GitLab	12	3%
5	TerraMaster	10	2%
6	Apple	13	3%
7	ASUSTOR	7	2%
8	WordPress	7	2%
9	Apache	6	1%
10	其他	278	67%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，40 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 WebKit 内存破坏漏洞（CNVD-2018-26502）、Google Android 权限提升漏洞（CNVD-2018-26777）”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/

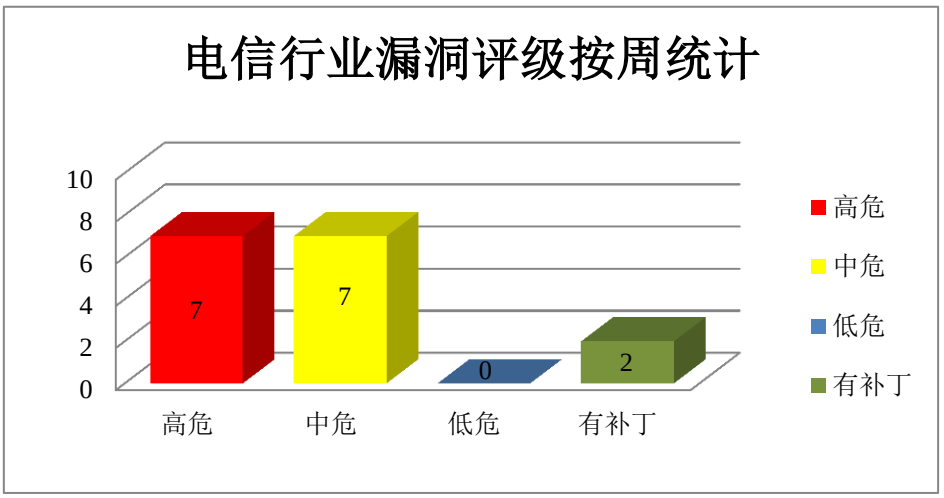

图 3 电信行业漏洞统计

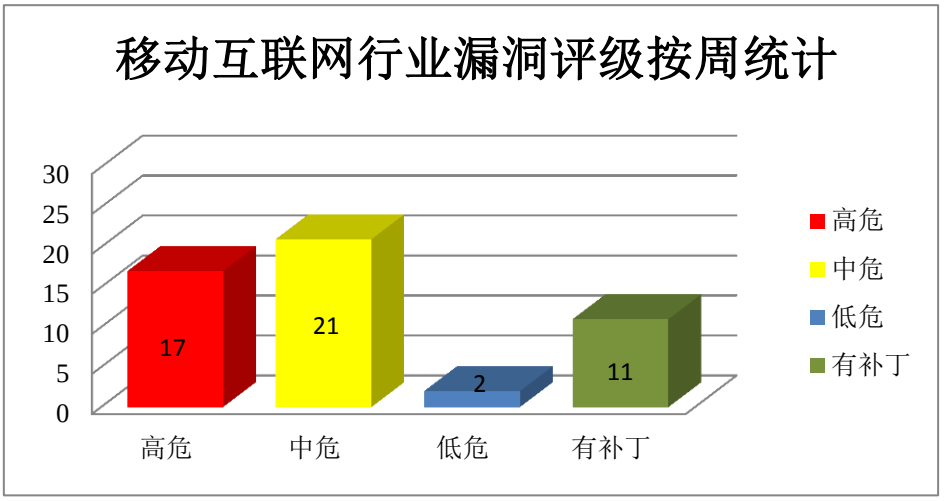

图 4 移动互联网行业漏洞统计

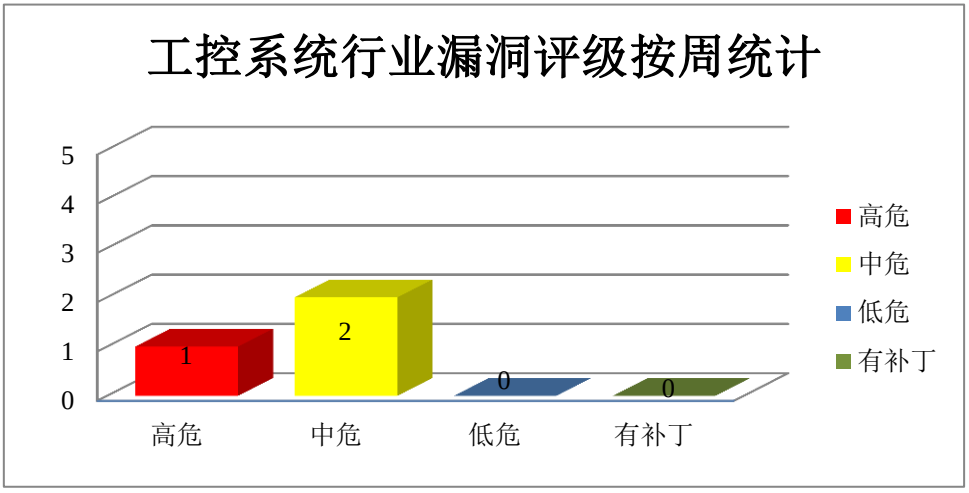

图 5 工控系统行业漏洞统计

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任意代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2018-26551、CNVD-2018-26552、CNVD-2018-26553、CNVD-2018-26554、CNVD-2018-26555、CNVD-2018-26556、CNVD-2018-26559、CNVD-2018-26560）。上述漏洞的综合评级为为“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-2018-26551
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26552
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26553
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26554
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26555
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26556
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26559
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26560

2、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft ChakraCore 是一个 Edge（Web 浏览器）所使用的 JavaScript 引擎的核心部分。Internet Explorer（IE）是其中的一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限，执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2018-26972、CNVD-2018-26971）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2018-26979）、Microsoft Windows Registry 本地权限提升漏洞、Microsoft Windows MS XML 远程执行代码漏洞、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2018-26985、CNVD-2018-26987）、Microsoft ChakraCore 和 Windows Edge 远程代码执行漏洞。上述漏洞的综合评级为为“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-2018-26972
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26971

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26979

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26978

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26980

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26985

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26987

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26986

3、IBM 产品安全漏洞

IBM DataPower Gateway 是一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台。MQ Appliance 是一款用于快速部署企业级消息中间件的一体机设备。IBM Connections 是一套社交软件平台。IBM Marketing Platform 是一套营销平台。IBM Security Guardium 是一套提供数据保护功能的平台。IBM BigFix Platform 是一套动态的集成了消息内容驱动和管理系统的多技术平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息或消耗内存资源等。

CNVD 收录的相关漏洞包括：IBM DataPower Gateway 和 MQ Appliance 拒绝服务漏洞、IBM Connections 信息泄露漏洞（CNVD-2018-26361）、IBM Marketing Platform XML 外部实体注入漏洞（CNVD-2018-26362、CNVD-2018-26364）、IBM DataPower Gateway 信息泄露漏洞（CNVD-2018-26363）、IBM Security Guardium 信息泄露漏洞（CNVD-2018-26895）、IBM Operational Decision Manager XML 外部实体注入漏洞（CNVD-2018-26896）、IBM BigFix Platform 信息泄露漏洞（CNVD-2018-26899）。其中，“IBM Marketing Platform XML 外部实体注入漏洞（CNVD-2018-26362、CNVD-2018-26364）、IBM Operational Decision Manager XML 外部实体注入漏洞（CNVD-2018-26896）”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-2018-26359

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26361

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26362

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26364

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26363

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26895

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26896

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26899

4、Apple 品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。WebKit 是 KDE、苹果（Apple）、谷歌（G

oogle）等公司共同开发的一套开源 Web 浏览器引擎，目前被 Apple Safari 及 Google Chrome 等浏览器使用。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple macOS Sierra 是为 Mac 计算机所开发的一套专用操作系统。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，伪造 UI，提升权限，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple macOS Mojave Intel Graphics Driver 未初始化内存信息泄露漏洞、Apple iOS libxpc 权限提升漏洞、多款 Apple 产品 WebKit 拒绝服务漏洞（CNVD-2018-26497）、Apple macOS Security 拒绝服务漏洞、Apple macOS Spotlight 内存破坏漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-26502）、Apple iOS Messages UI 欺骗漏洞（CNVD-2018-26503、CNVD-2018-26504）。其中，“Apple macOS Spotlight 内存破坏漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-26502）”的综合评级为为“高危”。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-2018-26495
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26496
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26497
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26500
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26501
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26502
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26503
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26504

5、ASUS Aura Sync 任意代码执行漏洞

ASUS Aura Sync 是一套灯效管理软件。本周，ASUS Aura Sync 被披露存在任意代码执行漏洞。本地攻击者可利用该漏洞执行任意的 ring-0 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-2018-26456

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-2018-26464	Zoho ManageEngine OpManager SQL 注入漏洞（CNVD-2018-26464）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.manageengine.co.uk/network-monitoring/help/read-me.html
CNVD-2018-26466	Chamilo LMS SQL 注入漏洞（CNVD-2018-26466）	高	厂商已发布漏洞修复程序，请及时关注更新：

			https://github.com/chamilo/chamilo-lms/commit/bfa1eccfabb457b800618d9d115f12dc614a55df
CNVD-2018-26638	Wireshark 拒绝服务漏洞（CNVD-2018-26638）	高	厂商已发布漏洞修复程序，请及时关注更新：https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=9c8645ec7b28e4d7193962ecd2a418613bf6a84f
CNVD-2018-26667	NVIDIA GeForce Experience 权限提升漏洞（CNVD-2018-26667）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.geforce.com/geforce-experience/download
CNVD-2018-26700	QNAP QTS 缓冲区溢出漏洞（CNVD-2018-26700）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.qnap.com/zh-tw/security-advisory/nas-201809-20
CNVD-2018-26782	ESTsoft ALZip 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://www.altools.co.kr/Support/Notice_Contents.aspx?idx=1677&page=2&t=
CNVD-2018-26795	Logitech Harmony Hub 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.myharmony.com/en-de/release-notes
CNVD-2018-26796	Netatalk 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://netatalk.sourceforge.net/3.1/ReleaseNotes3.1.12.html
CNVD-2018-26908	Linux kernel 越界访问漏洞（CNVD-2018-26908）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b799207e1e1816b09e7a5920fbb2d5fcf6edd681
CNVD-2018-26927	ASUSTOR ADM 操作系统命令注入漏洞（CNVD-2018-26927）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.asustor.com/adm/adm3_0

小结：本周，Adobe 被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Microsoft、IBM、Apple 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，伪造 UI，提升权限，执行任意代码，破坏内存，发起拒绝服务攻击等。另外，ASUS Aura Sync 被披露存在任意代码执行漏洞。本地攻击者可利用该漏洞执行任意的 ring-0 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、libxls 拒绝服务漏洞

验证描述

libxls 是一个用于读取 Exce（xls）文件的 C 语言库。

libxls 1.4.0 版本中的 ole.c 文件的‘read_MSAT_body’函数存在拒绝服务漏洞，攻击者可借助特制的文件利用该漏洞造成拒绝服务（应用程序崩溃）。

验证信息

POC 链接：https://github.com/evanmiller/libxls/issues/35

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-26647

信息提供者

恒安嘉新(北京)科技股份公司

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. WibuKey 云中存在漏洞，可执行代码

WibuKey 数字版权管理（DRM）解决方案中存在漏洞，该漏洞可被用来在受感染系统上披露信息，提升权限，甚至执行代码。适用于多种接口与操作系统的 WibuKey 广泛应用于 Straton、 Archicad,、GRAPHISOFT、V-Ray 及大量其他解决方案中。不过，Wibu Systems 建议新项目改用其公司的其他技术。在 DRM 解决方案中共发现了三个漏洞，这三个漏洞允许黑客在未授权的情况下读取内核内存信息，提升在本地系统的权限，且还可能允许黑客在可用的 WibuKey 网络服务器上执行代码。

参考链接：https://www.easyaq.com/news/348668036.shtml

2. Android 自带浏览器会泄露系统敏感信息

某网络安全咨询公司发现，谷歌的 Chrome 浏览器、WebView 和 Android 的 Chrome 标签显示了有关运行它的设备的硬件型号，固件版本和安全补丁级别的信息。这也会影响使用 Chrome 呈现网络内容的所有 Android 应用程序。此信息可用于跟踪用户和指纹设备。它还可用于确定特定设备易受攻击的漏洞，以便针对攻击。虽然供应商（Google）在 2015 年拒绝了最初的错误报告，但他们已于 2018 年 10 月针对 Chrome v70 发布了部分修复程序。该修复程序隐藏固件信息，同时保留硬件模型标识符。所有先前版本都会受到影响。建议用户升级到 70 或更高版本。由于此修复程序不适用于 WebView

用法，因此应用程序开发人员应手动覆盖其应用程序中的用户代理配置。

参考链接：https://www.freebuf.com/news/193168.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