国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 01 月 14 日-2019 年 01 月 20 日 **2019 年第 3 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 375 个，其中高危漏洞 110 个、中危漏洞 236 个、低危漏洞 29 个。漏洞平均分值为 5.86。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“Dolibarr ERP-CRM 'rowid' SQL 注入漏洞、Ampache 存在多个反射型跨站脚本漏洞”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 1501 个，与上周（1475 个）环比增长 2%。

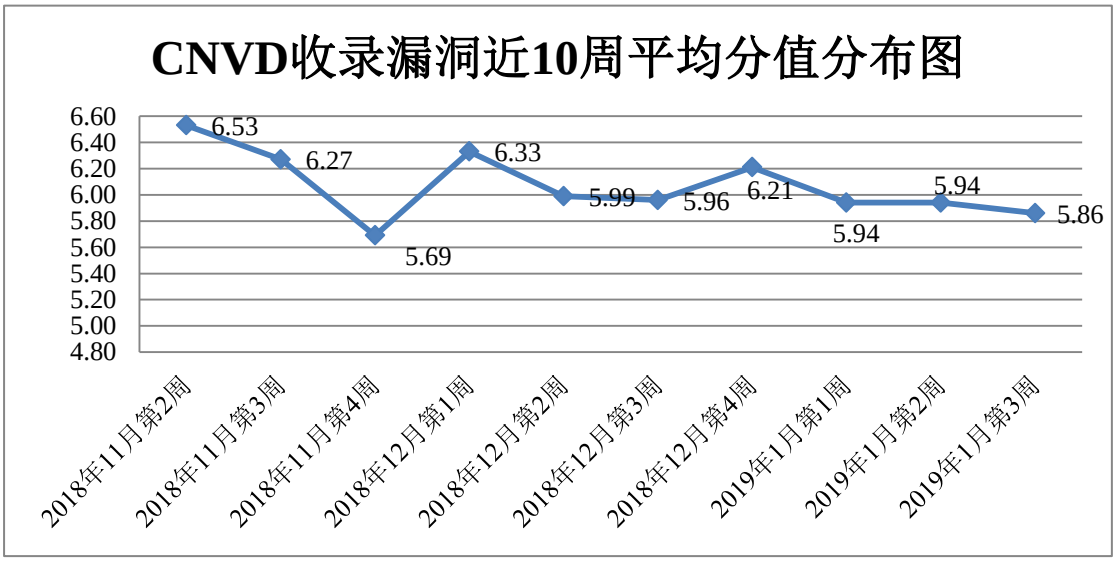

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 起，向银行、保险、能源等重要行业单位通报漏洞事件 17 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 253 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 103 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 9 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：

上海卓卓网络科技有限公司、武汉达梦数据库有限公司、北京锐和恒泰科技有限公司、沧州市凡诺广告传媒有限公司、深圳市圆梦云科技有限公司、中山市商友网络科技有限公司、深圳市凌盟科技有限公司、上海丹帆网络科技有限公司、济南白菜网络技术有限公司、老班 CMS、雷风影视、zzzcms、Wordpress。

本周，CNVD 发布了《Oracle 发布 2019 年 1 月的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4865

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、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。天津市国瑞数码安全系统股份有限公司、山东云天安全技术有限公司、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、南京联成科技发展股份有限公司、任子行网络技术股份有限公司、北京圣博润高新技术股份有限公司、广州竞远安全技术股份有限公司、河南信安世纪科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京安华金和科技有限公司、北京安信天行科技有限公司、北京国舜科技股份有限公司、上海零盾网络科技有限公司及其他个人白帽子向 CNVD 提交了 1475 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 926 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）	369	369
360 网神（补天平台）	353	353
新华三技术有限公司	297	0
哈尔滨安天科技集团股份有限公司	278	0
北京天融信网络安全技术有限公司	265	4
华为技术有限公司	205	0

北京数字观星科技有限公司	90	0
北京神州绿盟科技有限公司	69	0
中国电信集团系统集成有限责任公司	67	2
深信服科技股份有限公司	18	0
北京启明星辰信息安全技术有限公司	66	5
恒安嘉新(北京)科技股份公司	45	0
杭州安恒信息技术股份有限公司	1	1
北京知道创宇信息技术有限公司	1	0
天津市国瑞数码安全系统股份有限公司	400	400
山东云天安全技术有限公司	68	68
中新网络信息安全股份有限公司	55	55
安徽锋刃信息科技有限公司	44	44
南京联成科技发展股份有限公司	29	29
任子行网络技术股份有限公司	20	20
北京圣博润高新技术股份有限公司	8	8
广州竞远安全技术股份有限公司	6	6
河南信安世纪科技有限公司	4	4
远江盛邦（北京）网络安全科技股份有限公司	2	2
北京安华金和科技有限公司	1	1
北京安信天行科技有限公司	1	1
北京国舜科技股份有限公司	1	1
上海零盾网络科技有限公司	1	1

CNCERT 上海分中心	6	6
CNCERT 天津分中心	3	3
CNCERT 河北分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 宁夏分中心	1	1
个人	113	113
报送总计	2891	1501

本周漏洞按类型和厂商统计

本周，CNVD 收录了 375 个漏洞。应用程序漏洞 219 个，WEB 应用漏洞 75 个，操作系统漏洞 41 个，网络设备漏洞 35 个，安全产品漏洞 4 个，数据库漏洞 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
应用程序漏洞	219
WEB 应用漏洞	75
操作系统漏洞	41
网络设备漏洞	35
安全产品漏洞	4
数据库漏洞	1

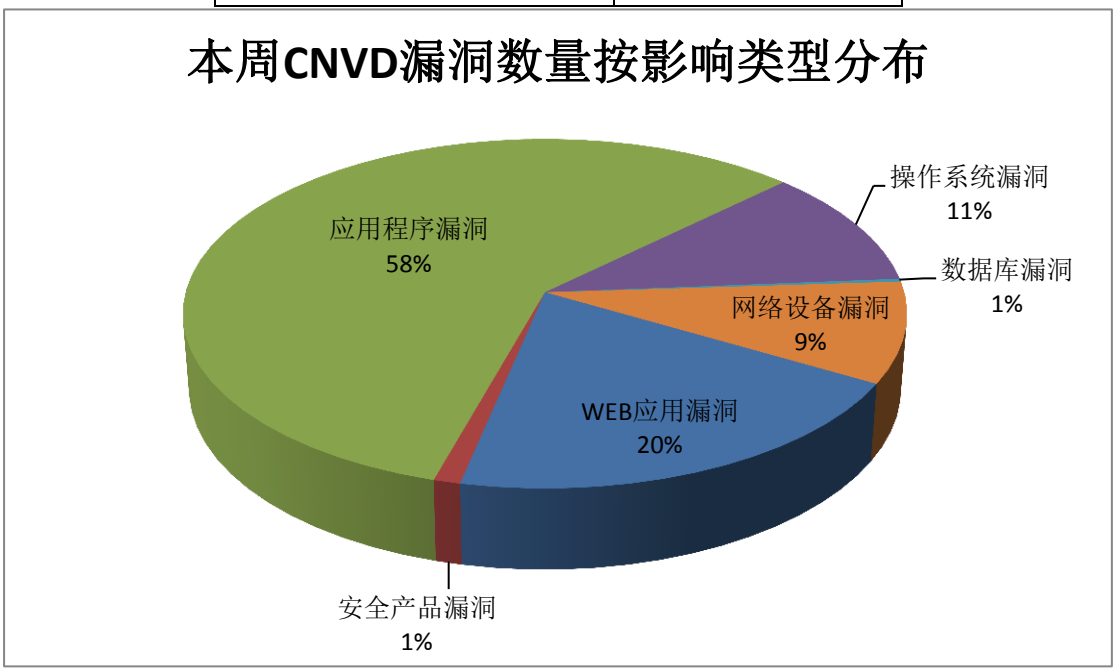

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、Apple 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	Google	61	16 %
2	Cisco	30	8%
3	Apple	18	5%
4	NEC	17	5%
5	Adobe	14	4%
6	PHPMyWind	11	3%
7	SemCms	10	3%
8	CloudBees	9	2%
9	WordPress	8	2%
10	其他	197	52%

本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，26 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，“Google Android 越界写入漏洞（CNVD-2019-01566）、Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2019-01903）、Google Android Kernel 权限提升漏洞（CNVD-2019-01596）、Omron CX-One CX-Protocol 任意代码执行漏洞”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/

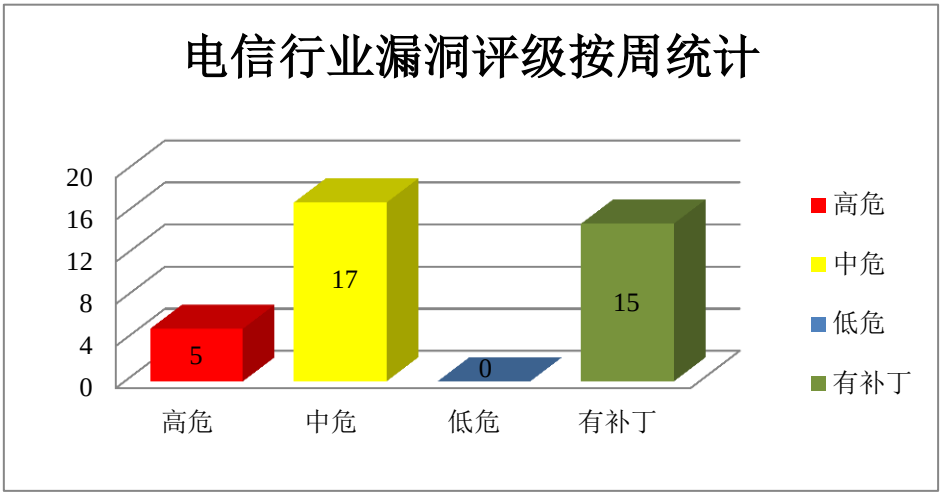

图 3 电信行业漏洞统计

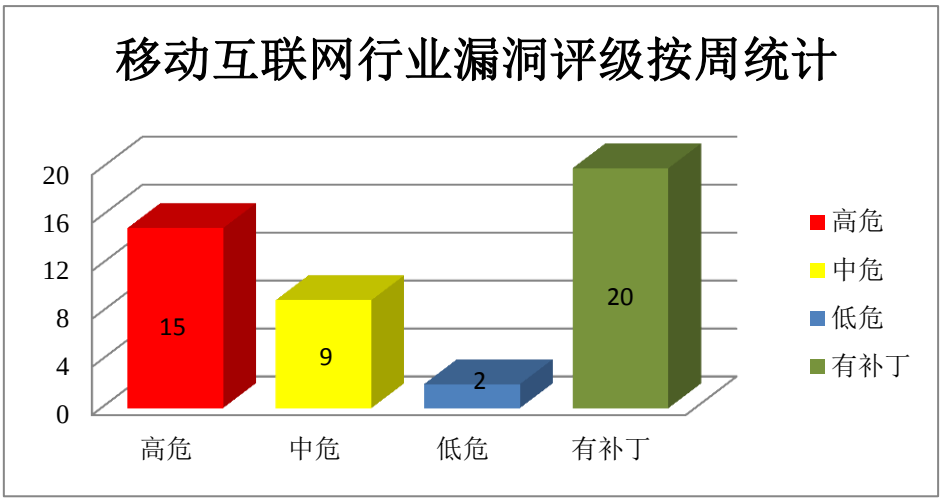

图 4 移动互联网行业漏洞统计

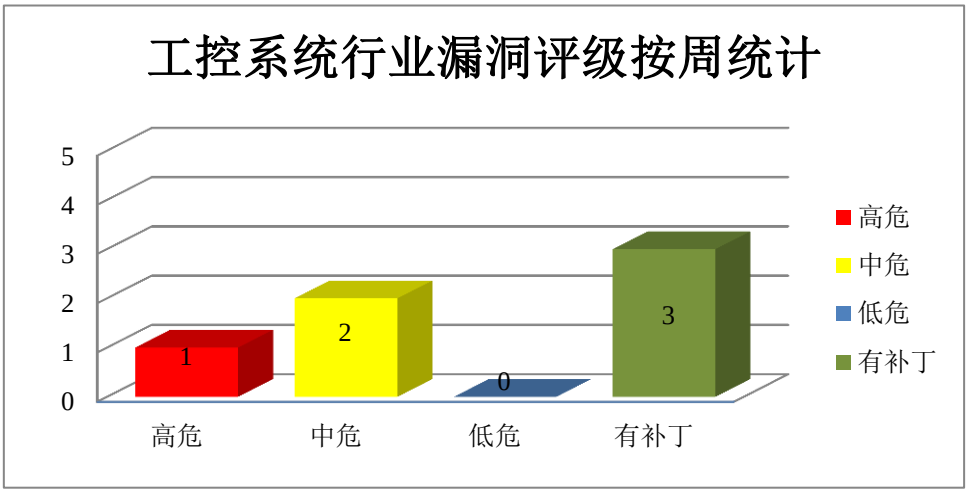

图 5 工控系统行业漏洞统计

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 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越界读取漏洞，攻击者可利用漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-01912、CNVD-2019-01913、CNVD-2019-01914、CNVD-2019-01915、CNVD-2019-01916、CNVD-2019-01917、CNVD-2019-01918、CNVD-2019-01919）。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-2019-01912
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01913
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01914
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01915
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01916
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01917
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01918
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01919

2、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome V8 缓冲区溢出漏洞（CNVD-2019-01111）、Google Chrome WebAssembly 代码执行漏洞、Google Android 越界写入漏洞（CNVD-2019-01560、CNVD-2019-01561）、Google Android Kernel 权限提升漏洞（CNVD-2019-01596）、Google Android 远程代码执行漏洞（CNVD-2019-01597、CNVD-2019-01598、CNVD-2019-01601）。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-2019-01111
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01112
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01560
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01561
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01596
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01597
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01598
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01601

3、Cisco 产品安全漏洞

Cisco Email Security Appliance(ESA)是一个电子邮件安全设备。AsyncOS Software 是使用在其中的操作系统。Cisco Integrated Management Controller（IMC）Supervisor 是一套用于对 UCS（统一计算系统）进行管理的工具，它支持 HTTP、SSH 访问等，并可对服务器进行开机、关机和重启等操作。Cisco Registered Envelope Service 是一套邮件服务解决方案。Cisco Adaptive Security Appliances（ASA，自适应安全设备）Software 是一套运行于防火墙中的操作系统。Cisco Firepower Threat Defense（FTD）Software 一套提供下一代防火墙服务的统一软件。Cisco IOS Software 和 IOS XE Software 都是为其网络设备开发的操作系统。Cisco Prime Collaboration Assurance（PCA）是一套企业协作网络管理解决方案。Cisco IOS Access Points（APs）Software 是一套用于管理控制访问接入点设备的软件。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，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Email Security Appliance S/MIME 拒绝服务漏洞、Cisco Policy Suite for Mobile 和 Policy Suite Diameter Routing Agent 访问绕过漏洞、Cisco Integrated Management Controller Supervisor SQL 注入漏洞、Cisco Registered Envelope Service 信息泄露漏洞、Cisco Adaptive Security Appliance Software 和 Cisco Firepower Threat Defense Software 拒绝服务漏洞、Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2019-01903）、Cisco Prime Collaboration Assurance 跨站请求伪造漏洞（CNVD-2019-01908）、Cisco IOS Access Points Software 拒绝服务漏洞。其中，除“Cisco Registered Envelope Service 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-2019-01871

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01894

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01896

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01897

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01904

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01903

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01908

http://www.cnvd.org.cn/flaw/show/CNVD-2019-01928

4、Apple 品安全漏洞

Apple macOS Sierra、macOS High Sierra 和 macOS Mojave 都是美国苹果（Apple）公司为 Mac 计算机所开发的不同版本的专用操作系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，绕过管理员身份验证（无需管理员密码），执行任意代码。

CNVD 收录的相关漏洞包括：Apple macOS High Sierra AppleGraphicsPowerManagement 缓冲区溢出漏洞、Apple macOS High Sierra AppleGraphicsControl 缓冲区溢出漏洞、Apple macOS Sierra Remote Management 权限漏洞、Apple macOS High Sierra AMD 输入验证漏洞、Apple macOS High Sierra Security 逻辑缺陷漏洞、Apple macOS High Sierra Kernel 越界读取漏洞（CNVD-2019-01542）、Apple macOS High Sierra APFS 逻辑缺陷漏洞、Apple macOS Intel Graphics Driver 内存错误引用漏洞。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-2019-01533
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01534
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01535
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01539
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01541
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01542
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01548
http://www.cnvd.org.cn/flaw/show/CNVD-2019-01678

5、多款 Tenda 产品 httpd 缓冲区溢出漏洞（CNVD-2019-01888）

Tenda AC7 等都是中国腾达（Tenda）公司的无线路由器产品。httpd 是其中的一个 HTTP 服务器组件。本周，多款 Tenda 产品中的 httpd 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞造成拒绝服务（覆盖函数的返回值）。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-2019-01888

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-2019-01292	CloudBees Jenkins Email Extension Template Plugin 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jenkins.io/security/advisory/2018-09-25/#SECURITY-1125
CNVD-2019-01296	OpenSSH 访问限制绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2
CNVD-2019-01301	apex-publish-static-files npm 命令注入漏洞	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://github.com/vincentmorneau/apex-publish-static-files
CNVD-2019-01302	libnmapp package 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/jas-/node-libnmap/issues/54
CNVD-2019-01305	CIMTechniques CIMScan SQL 代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://cimtechniques.com/
CNVD-2019-01309	Foxit PDF SDK ActiveX 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxitsoftware.com/support/security-bulletins.php
CNVD-2019-01310	Foxit PDF SDK ActiveX 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://www.foxitsoftware.com/support/security-bulletins.php
CNVD-2019-01321	LogonTracer 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/JPCERTCC/LogonTracer/releases/tag/v1.2.1
CNVD-2019-01319	LogonTracer 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://github.com/JPCERTCC/LogonTracer/releases/tag/v1.2.1
CNVD-2019-01682	Omron CX-One CX-Protocol 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.omron.com/

小结：本周，Adobe 被披露存在越界读取漏洞，攻击者可利用漏洞获取敏感信息。此外，Google、Cisco、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，升权限，绕过管理员身份验证（无需管理员密码），执行任意代码，发起拒绝服务攻击等。另外，多款 Tenda 产品 httpd 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞造成拒绝服务（覆盖函数的返回值）。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、Dolibarr ERP-CRM 'rowid' SQL 注入漏洞

验证描述

Dolibarr ERP/CRM 是法国 Dolibarr 基金会的一套基于 Web 的企业资源计划（ERP）

和客户关系管理（CRM）系统。该系统可用来管理产品、库存、发票、订单等。

Dolibarr ERP-CRM 'rowid' SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=31909

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-01712

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. ES 文件管理器现严重漏洞，建议用户及时更新

近日，一款知名软件 ES 文件管理器被曝出有重大漏洞，能够导致用户手机上的文件泄漏给同一网络下的所有用户。目前新版本已经在 Google Play 上架，版本号为 v4.1.9.9，更新日志有明确提到“修复局域网内 http 漏洞”。建议所有使用旧版本的用户及时更新到最新的版本，以防止手机中重要信息泄露。

参考链接：https://www.freebuf.com/news/194646.html

2. Amadeus 航班预订系统存在严重漏洞

以色列安全研究员 Noam Rotem 在预定以色列航空公司的航班时发现了 Amadeus 在线机票预订系统中的一个严重漏洞，该漏洞使得攻击者能够远程访问和修改用户的行程细节并获得他们的飞行常客里程。攻击者只要知道受害者的 PNR（乘客姓名记录）号码即可利用此漏洞。

参考链接：https://securityaffairs.co/wordpress/79972/hacking/amadeus-flight-booking-system-bug.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