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 17 日-2018 年 12 月 23 日 **2018 年第 51 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 352 个，其中高危漏洞 137 个、中危漏洞 174 个、低危漏洞 41 个。漏洞平均分值为 5.96。本周收录的漏洞中，涉及 0day 漏洞 243 个（占 69%），其中互联网上出现“UltraISO 'Output FileName'拒绝服务漏洞、WordPress 插件 JoeBooking 信息泄露漏洞”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 1991 个，与上周（1213 个）环比增长 64%。

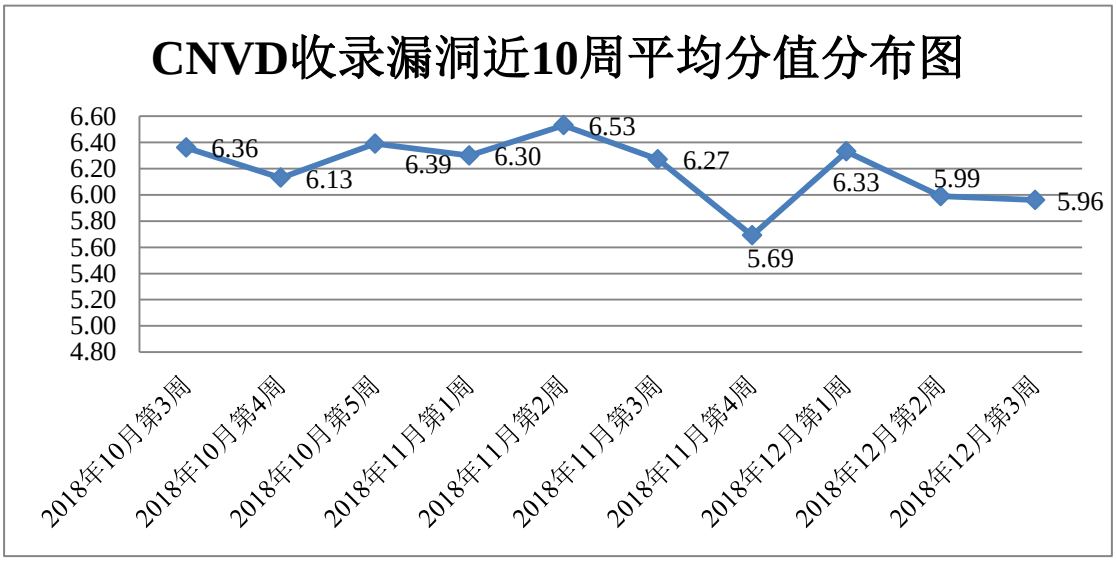

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 12 起，向银行、保险、能源等重要行业单位通报漏洞事件 37 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 265 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 91 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 22 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：

济南考源信息科技有限公司、洪湖尔创网联信息技术有限公司、智士软件（北京）有限公司、江苏连邦信息技术有限公司、镇江市云优网络科技有限公司、漳州豆壳网络科技有限公司、南京金鹊软件科技有限公司、湖南第五元素网络科技开发有限公司、济南泰创软件科技有限公司、成都市唯美互动网络科技有限公司、北京思纽教育科技有限公司、苏州市艾特信息技术有限公司、信呼、雷风影视、DM 建站系统、Elefant CMS、HuCart、EARCLINK、Zzzcms、ZZCMS、ITKEE 等 25 家网站和厂商软件产品漏洞。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，沈阳东软系统集成工程有限公司、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、中国电信集团系统集成有限责任公司、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。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、南京联成科技发展股份有限公司、北京国舜科技股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、任子行网络技术股份有限公司、浙江大华技术股份有限公司、上海银基信息安全技术股份有限公司、河南信安世纪科技有限公司、内蒙古奥创科技有限公司、成都思维世纪科技有限公司、海南上德科技有限公司、山石网科通信技术有限公司、北京信联科汇科技有限公司及其他个人白帽子向 CNVD 提交了 1991 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 1464 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）	866	866
360 网神（补天平台）	598	598
沈阳东软系统集成工程有限公司	358	0
北京天融信网络安全技术有限公司	199	3
哈尔滨安天科技集团股份有限公司	176	0

中国电信集团系统集成有限责任公司	144	4
北京神州绿盟科技有限公司	136	0
新华三技术有限公司	123	0
华为技术有限公司	121	0
北京数字观星科技有限公司	115	0
北京启明星辰信息安全技术有限公司	80	0
恒安嘉新(北京)科技股份公司	49	0
西安四叶草信息技术有限公司	22	22
深信服科技股份有限公司	16	0
杭州安恒信息技术股份有限公司	3	3
北京知道创宇信息技术有限公司	2	0
山东云天安全技术有限公司	85	85
安徽锋刃信息科技有限公司	45	45
中新网络信息安全股份有限公司	43	43
北京圣博润高新技术股份有限公司	21	21
南京联成科技发展股份有限公司	19	19
北京国舜科技股份有限公司	10	10
远江盛邦（北京）网络安全科技股份有限公司	9	9
任子行网络技术股份有限公司	8	8
浙江大华技术股份有限公司	8	8
上海银基信息安全技术股份有限公司	7	7
河南信安世纪科技有限公司	6	6

内蒙古奥创科技有限公司	4	4
成都思维世纪科技有限公司	2	2
海南上德科技有限公司	2	2
山石网科通信技术有限公司	1	1
北京信联科汇科技有限公司	1	1
CNCERT 湖南分中心	14	14
CNCERT 贵州分中心	8	8
CNCERT 上海分中心	5	5
CNCERT 河北分中心	4	4
CNCERT 黑龙江分中心	4	4
CNCERT 吉林分中心	4	4
CNCERT 天津分中心	3	3
CNCERT 甘肃分中心	2	2
CNCERT 浙江分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 新疆分中心	1	1
个人	176	176
报送总计	3503	1991

本周漏洞按类型和厂商统计

本周，CNVD 收录了 352 个漏洞。WEB 应用漏洞 143 个，应用程序漏洞 142 个，操作系统漏洞 29 个，网络设备漏洞 28 个，数据库漏洞 5 个，安全产品漏洞 5 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
WEB 应用漏洞	143
应用程序漏洞	142

操作系统漏洞	29
网络设备漏洞	28
数据库漏洞	5
安全产品漏洞	5

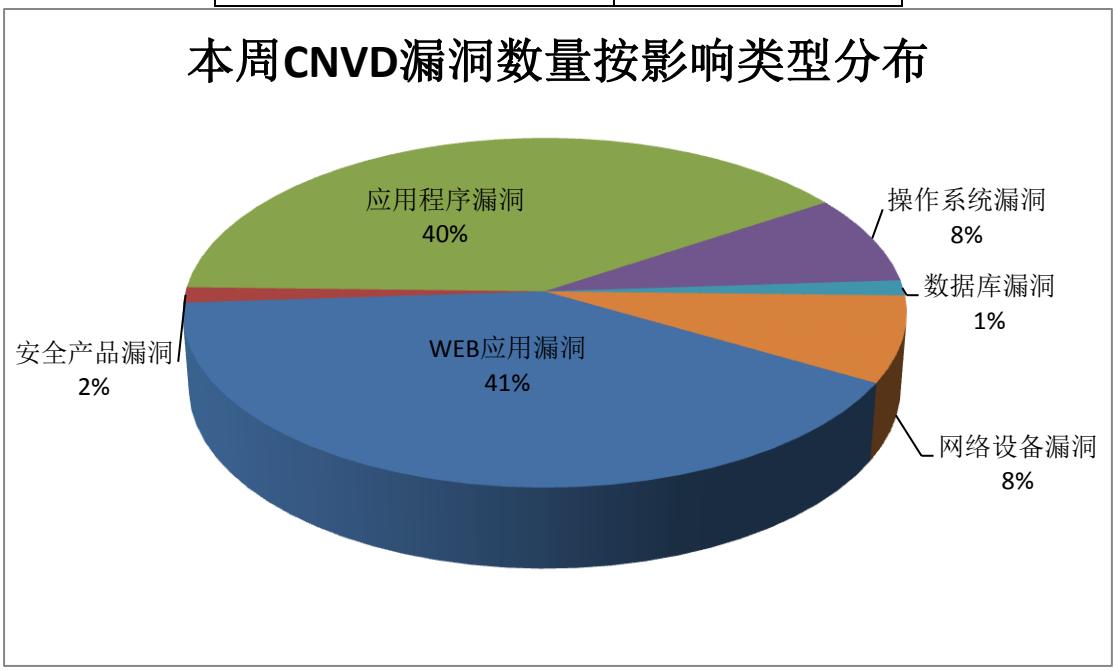

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Apple、Google 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	24	7%
2	Apple	20	6%
3	Google	10	3%
4	Mozilla	10	3%
5	WordPress	8	2%
6	Intel	5	1%
7	Samsung	5	1%
8	TRENDnet	5	1%
9	Adobe	5	1%
10	其他	260	75%

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洞，13 个工控行业漏洞（如下图所示）。其中，“Google Android Library 远程代码执行漏洞、Apple iOS、tvOS 和 macOS Mojave Airport 类型混淆漏洞、Google Android Runtime 权限提升漏洞（CNVD-2018-26250）、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-25679）”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/

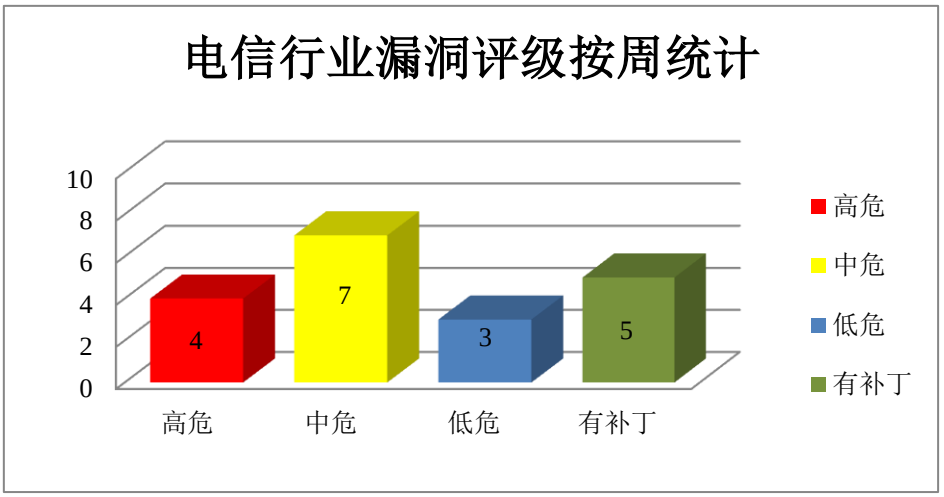

图 3 电信行业漏洞统计

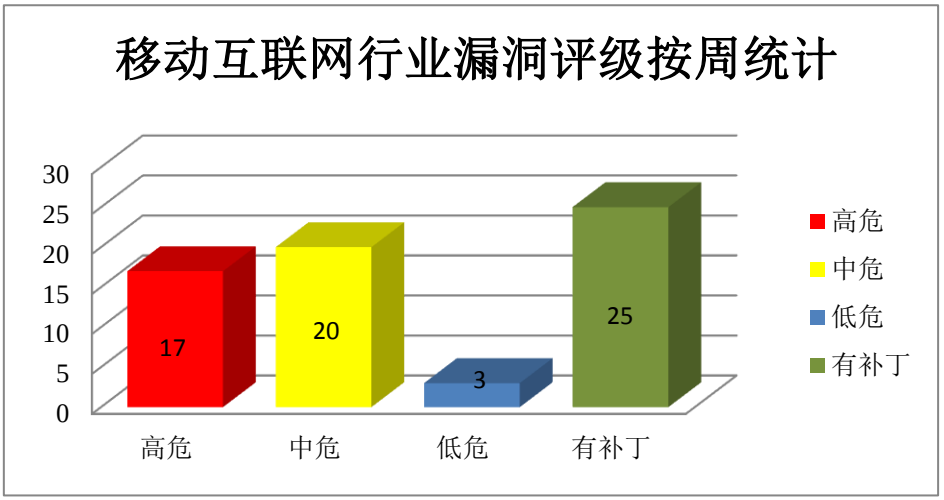

图 4 移动互联网行业漏洞统计

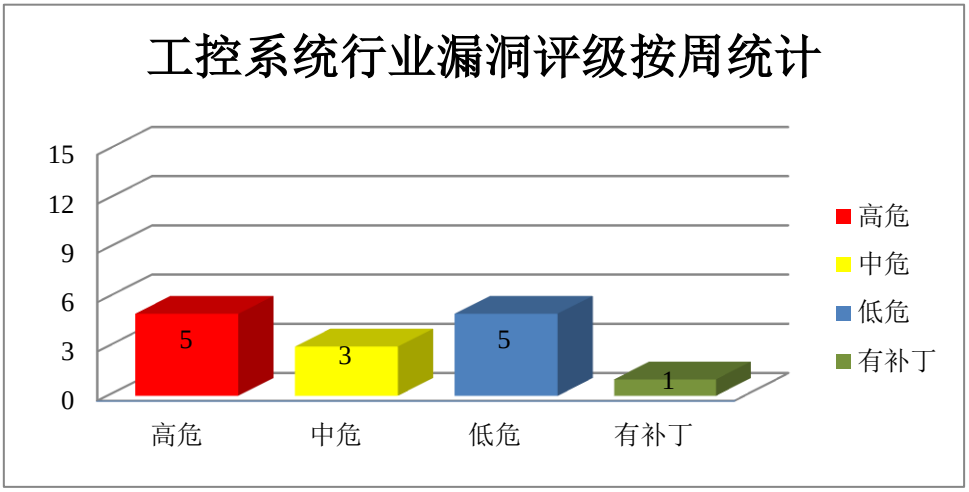

图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

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。tvOS 是一套智能电视操作系统；macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。本周，上述产品被披露存在内存破坏和类型混淆漏洞，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：多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-25673、CNVD-2018-25675、CNVD-2018-25679、CNVD-2018-25683、CNVD-2018-25684、CNVD-2018-25685、CNVD-2018-25687）、Apple iOS、tvOS 和 macOS Mojave Airport 类型混淆漏洞。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-2018-25673

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25675

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25679

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25683

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25684

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25685

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25687

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25676

2、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox 的一个延长支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，发起拒绝

服务攻击等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 缓冲区溢出漏洞（CNVD-2018-25859）、Mozilla Firefox 内存破坏漏洞（CNVD-2018-25860）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2018-25863）、Mozilla Firefox 未授权访问漏洞（CNVD-2018-25864）、Mozilla Firefox 和 Firefox ESR 整数溢出漏洞（CNVD-2018-25865）、Mozilla Firefox URI 限制绕过漏洞、Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2018-25867）、Mozilla Firefox 和 Firefox ESR 缓冲区溢出漏洞（CNVD-2018-25869）。其中，除“Mozilla Firefox 缓冲区溢出漏洞（CNVD-2018-25859）、Mozilla Firefox 未授权访问漏洞（CNVD-2018-25864）、Mozilla Firefox URI 限制绕过漏洞”外，其余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-2018-25859
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25860
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25863
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25864
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25865
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25866
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25867
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25869

3、Google 产品安全漏洞

Google Go 是一种针对多处理器系统应用程序的编程进行了优化的编程语言。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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Go 远程代码执行漏洞、Google Android Runtime 远程代码执行漏洞、Google Android Runtime 权限提升漏洞（CNVD-2018-26250）、Google Android Library 远程代码执行漏洞、Google Android Media Framework 拒绝服务漏洞（CNVD-2018-26252）、Google Android System 权限提升漏洞（CNVD-2018-26253、CNVD-2018-26254、CNVD-2018-26255）。其中，除“Google Android Media Framework 拒绝服务漏洞（CNVD-2018-26252）”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-2018-25737
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26249
http://www.cnvd.org.cn/flaw/show/CNVD-2018-26250

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26251

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26252

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26253

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26254

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26255

4、IBM 品安全漏洞

IBM Cloud Private 是一套企业私有云解决方案。IBM StoredIQ 是一套数据可视化处理平台。IBM API Connect（又名 APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM DB2 for Linux 是一套基于 Linux 平台的关系型数据库管理系统。IBM WebSphere Application Server（WAS）是一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。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，执行未授权操作，提升权限，造成拒绝服务。

CNVD 收录的相关漏洞包括：IBM Cloud Private 信息泄露漏洞（CNVD-2018-26025）、IBM StoredIQ 跨站请求伪造漏洞、IBM API Connect 拒绝服务漏洞（CNVD-2018-26026）、IBM DB2 for Linux 拒绝服务漏洞、IBM API Connect 身份验证绕过漏洞、IBM API Connect 权限提升漏洞、IBM WebSphere Application Server 权限提升漏洞（CNVD-2018-26217、CNVD-2018-26216）。其中，“IBM StoredIQ 跨站请求伪造漏洞、IBM API Connect 身份验证绕过漏洞、IBM API Connect 权限提升漏洞”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-2018-26025

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26023

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26026

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26035

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26185

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26186

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26217

http://www.cnvd.org.cn/flaw/show/CNVD-2018-26216

5、Philips iSite PACS 和 IntelliSpace PACS 访问绕过漏洞

Philips iSite PACS 和 IntelliSpace PACS 都是用于医疗行业的放射学影像管理系统。本周，Philips iSite PACS 和 IntelliSpace PACS 被披露存在访问绕过漏洞。攻击者可利用该漏洞控制系统的组件。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-2018-26105

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-2018-26257	Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2018-26257）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html
CNVD-2018-25745	Terminology 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.enlightenment.org/news/2018-12-16-terminology-1.3.1
CNVD-2018-25748	Moxa NPort W2x50A 操作系统命令注入漏洞	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://www.moxa.com/
CNVD-2018-25873	Bosch IP Camera 缓冲区溢出漏洞	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://www.boschsecurity.com/
CNVD-2018-26256	Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2018-26256）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html
CNVD-2018-25879	Webroot BrightCloud SDK 缓冲区溢出漏洞	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://www.brightcloud.com/
CNVD-2018-25883	Artifex Software Ghostscript 类型混淆漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=693baf02152119af6e6afd30bb8ec76d14f84bbf
CNVD-2018-25912	Siemens SIMATIC IT LMS、SIMATIC IT Production Suite 和 SIMATIC IT UA Discrete Manufacturing 授权问题漏洞	高	目前厂商只发布了 SIMATIC IT Production Suite 等产品的升级补丁以修复漏洞，产品 SIMATIC IT LMS 的升级补丁暂未发布，详情请参考链接：https://cert-portal.siemens.com/productcert/pdf/ssa-944083.pdf
CNVD-2018-26103	TIBCO MessagiTIBCO Messaging - Apache Kafka Distribution - Schema Repository 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tibco.com/support/advisories/2018/11/tibco-security-advisory-november-6-2018-tibco-messaging-apache-kafka-distribution-schema-repository
CNVD-2018-26259	Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2018-26259）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接: https://helpx.adobe.com/security/produc

			ts/acrobat/apsb18-30.html

小结：本周，Apple 被披露存在内存破坏和类型混淆漏洞，攻击者可利用漏洞提升权限，执行任意代码（内存破坏）。此外，Mozilla、Google、IBM 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，执行未授权操作，提升权限，执行任意代码，发起拒绝服务攻击等。另外，Philips iSite PACS 和 IntelliSpace PACS 被披露存在访问绕过漏洞。攻击者可利用该漏洞控制系统的组件。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、UltraISO 'Output FileName'拒绝服务漏洞

验证描述

UltraISO 是一款光盘映像 ISO 文件编辑制作工具。

UltraISO 'Output FileName'存在拒绝服务漏洞。攻击者可利用漏洞发起拒绝服务攻击。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=31737

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-25694

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. 罗技 Options 被曝漏洞可招致按键注入攻击，官方发新版软件修复

Logitech Options 是罗技官方推出的一款软件，用户可以使用它对罗技鼠标、键盘和触摸板进行自定义。今年 9 月，谷歌 Project Zero 的安全研究员 Tavis Ormandy 发现了这款软件上的一个漏洞，可以招致按键注入攻击。通过此漏洞，应用程序可以打开一个 WebSocket 服务器。通过这一方式，外部来源可以用最小限度的身份验证，从任意网站访问应用程序。攻击者可以通过流氓网站向 Options 应用程序发送一系列命令，更改用户的设置。此外，还可通过更改一些简单的配置设置，来发送任意击键命令，从而获得访问所有信息的方式，甚至接管目标设备。也就是说，只要用户的电脑处于打开状态，同时这一应用保持在后台运行，理论上攻击者几乎能发起连续访问。

参考链接：https://www.ithome.com/0/400/704.htm

2. Elasticsearch 核心插件 Kibana 本地文件包含漏洞分析

Elasticsearch Kibana 是荷兰 Elasticsearch 公司的一套开源的、基于浏览器的分析和搜索 Elasticsearch 仪表板工具，作为 Elasticsearch 的核心组件，Kibana 可作为产品或服务提供，并与各种系统，产品，网站和企业中的其他 Elastic Stack 产品配合使用。不久前 Elasticsearch 发布了最新安全公告， Elasticsearch Kibana 6.4.3 之前版本和 5.6.13 之前版本中的 Console 插件存在严重的本地文件包含漏洞可导致拒绝服务攻击、任意文件读取攻击、配合第三方应用反弹 SHELL 攻击。由于 Kibana 在大数据领域用途较为广泛，此次漏洞影响范围较大。

参考链接：https://www.anquanke.com/post/id/168291

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