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 03 日-2018 年 12 月 09 日 **2018 年第 49 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 244 个，其中高危漏洞 108 个、中危漏洞 110 个、低危漏洞 26 个。漏洞平均分值为 6.33。本周收录的漏洞中，涉及 0day 漏洞 113 个（占 46%），其中互联网上出现“Joomla Content Editor Com_JCE 组件信息泄露漏洞、Avahi 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 987 个，与上周（884 个）环比增长 12%。

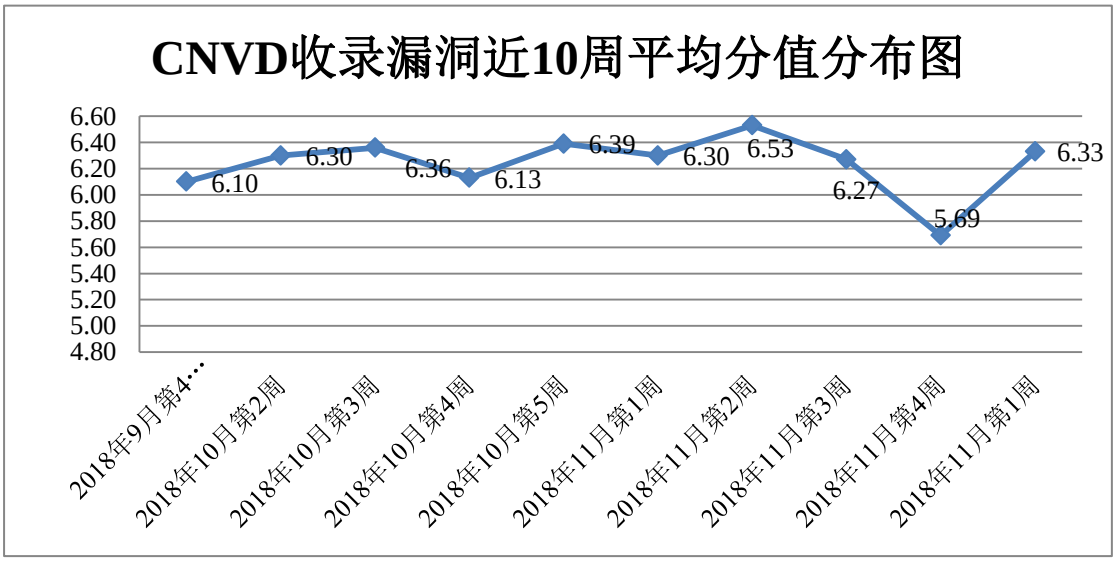

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 35 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 195 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 12 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：

成都康菲顿特网络科技有限公司、淄博闪灵网络科技有限公司、深圳市华企未来科技有限公司、北京字节跳动科技有限公司、友讯科技股份有限公司、邳州天目网络科技有限公司、上海亿速网络科技有限公司、北京印象笔记科技有限公司、深圳市锟铻科技有限公司、长沙翱云网络科技有限公司、国能日新科技股份有限公司、成都九安科技有限公司、云迈电子商务有限公司、酷溜网（北京）科技有限公司、广州齐博网络科技有限公司、北京夜猫网络科技有限公司、中国检验认证集团广西有限公司、北京汗青伟业科技有限公司、星际（杭州）网络技术有限公司、北京若深科技有限公司、金山软件股份有限公司、深圳市点晴信息技术有限公司、迈普通信技术股份有限公司、上海天泰网络技术有限公司、苏州德斯克信息技术有限公司、横河电机(中国)有限公司、合肥司瓦图网络科技有限责任公司、沧州市凡诺广告传媒有限公司、广西集翔网大信息科技有限公司、江苏国泰新点软件有限公司、成都爱诚科技有限公司、广州瀚德网络科技有限公司、济南政和科技有限公司、桂林英泰商务有限公司、杭州乐邦科技有限公司、南大傲拓科技江苏有限公司、灵吉网络科技有限公司、深圳市盛世桃源网络科技有限公司、北京联达动力信息科技股份有限公司、苏州烟火网络科技有限公司、深圳市明天见科技有限公司、阳光印网、雷风影视、为因软件、安米程序、YCCMS、HuCart、PHPMyWind、NEO、HuCart。

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、华为技术有限公司、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、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。广州竞远安全技术股份有限公司、安徽锋刃信息科技有限公司、北京国舜科技股份有限公司、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、山东云天安全技术有限公司、内蒙古奥创科技有限公司、南京联成科技发展股份有限公司、河南信安世纪科技有限公司、山石网科通信技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、新疆海狼科技有限公司、中移（杭州）信息技术有限公司及其他个人白帽子向 CNVD 提交了 987 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 625 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）	426	426
新华三技术有限公司	210	0
华为技术有限公司	202	0
斗象科技（漏洞盒子）	199	199
哈尔滨安天科技集团股份有限公司	194	0
北京天融信网络安全技术有限公司	85	22
中国电信集团系统集成有限责任公司	70	3
北京神州绿盟科技有限公司	65	0
北京数字观星科技有限公司	59	0
恒安嘉新(北京)科技股份公司	54	0
深信服科技股份有限公司	20	0
北京知道创宇信息技术有限公司	10	0
沈阳东软系统集成工程有限公司	4	4
杭州安恒信息技术股份有限公司	3	3
南京铱迅信息技术股份有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
广州竞远安全技术股份有限公司	36	36
安徽锋刃信息科技有限公司	35	35
北京国舜科技股份有限公司	31	31
中新网络信息安全股份有限公司	30	30
北京圣博润高新技术股份有限公司	21	21
山东云天安全技术有限公司	20	20

内蒙古奥创科技有限公司	7	7
南京联成科技发展股份有限公司	6	6
河南信安世纪科技有限公司	2	2
山石网科通信技术有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
新疆海狼科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 甘肃分中心	11	11
CNCERT 新疆分中心	6	6
CNCERT 上海分中心	2	2
CNCERT 贵州分中心	1	1
个人	116	116
报送总计	1931	987

本周漏洞按类型和厂商统计

本周，CNVD 收录了 213 个漏洞。应用程序漏洞 114 个，WEB 应用漏洞 64 个，操作系统漏洞 54 个，安全产品漏洞 6 个，网络设备漏洞 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	114
WEB 应用漏洞	64
操作系统漏洞	54
安全产品漏洞	6
网络设备漏洞	6

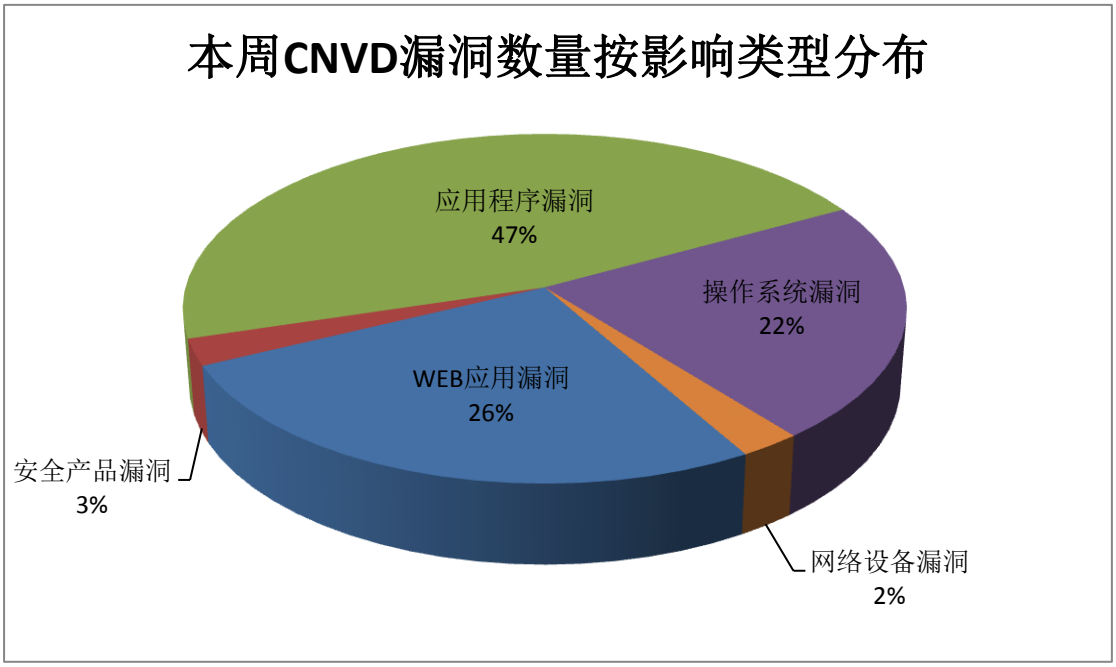

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Apple、Linux 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	38	16%
2	Apple	29	12%
3	Linux	23	9%
4	Foxit	7	3%
5	HDCMS	4	2%
6	Qualcomm	4	2%
7	LaySNS	3	1%
8	Ricoh	3	1%
9	YCCMS	3	1%
10	其他	130	53%

本周行业漏洞收录情况

本周，CNVD 收录了 5 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，“多款 Apple 产品 Kernel 内存破坏漏洞（CNVD-2018-24791）、Apple iOS 和 macOS Disk Images 内存破坏漏洞、Apple iOS、tvOS 和 macOS Mojave Kernel

权限提升漏洞”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/

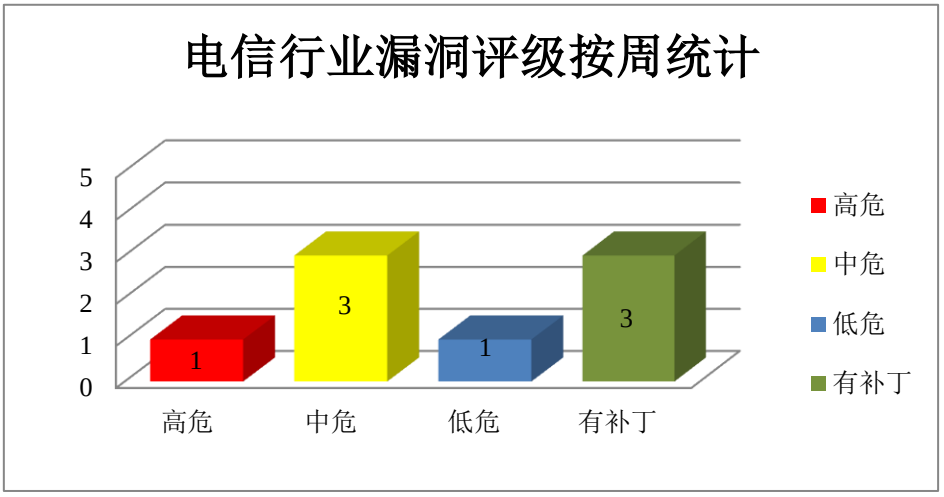

图 3 电信行业漏洞统计

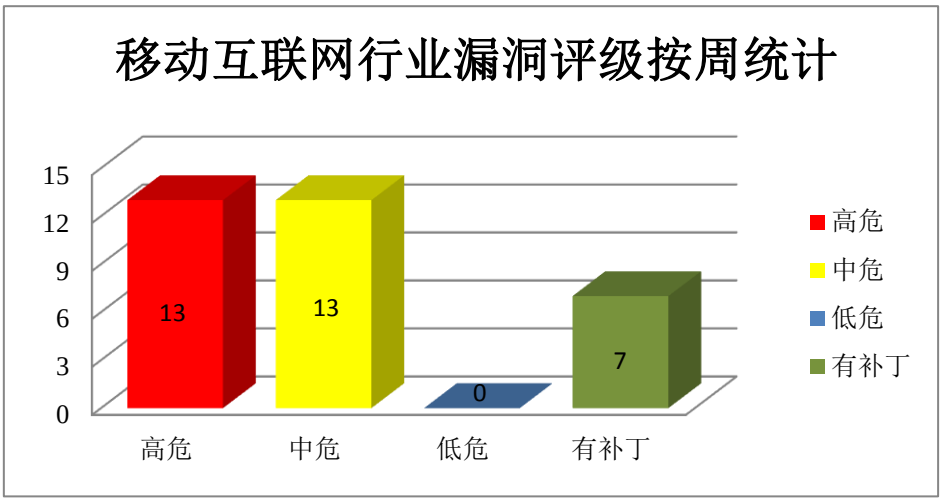

图 4 移动互联网行业漏洞统计

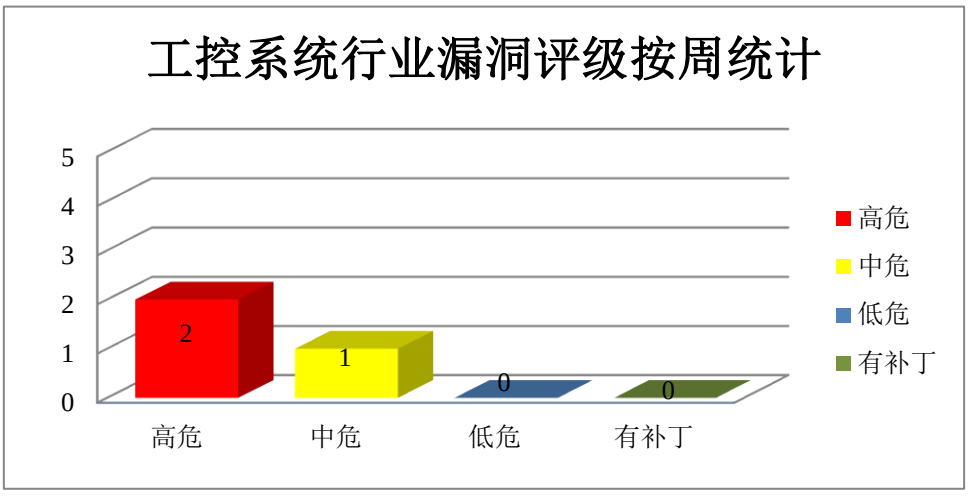

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM QRadar SIEM 是一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM WebSphere Cast Iron 是一款基于云计算的软件。IBM Security Identity Governance and Intelligence（IGI）是一套身份管理和治理解决方案。IBM QRadar SIEM 是一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM QRadar Incident Forensics 是一套安全取证调查软件。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，执行任意命令或发起拒绝服务攻击（消耗内存资源）。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM XML 外部实体注入漏洞（CNVD-2018-24553）、IBM WebSphere Cast Iron 信息泄露漏洞、IBM Security Identity Governance and Intelligence 信息泄露漏洞（CNVD-2018-24621、CNVD-2018-24622、CNVD-2018-24624、CNVD-2018-24627）、IBM QRadar SIEM OS 命令注入漏洞（CNVD-2018-24637）、IBM QRadar Incident Forensics 拒绝服务漏洞。其中，“IBM QRadar SIEM XML 外部实体注入漏洞（CNVD-2018-24553）、IBM WebSphere Cast Iron 信息泄露漏洞、IBM QRadar SIEM OS 命令注入漏洞（CNVD-2018-24637）”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-2018-24553

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24619

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24621

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24622

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24624

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24627

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24637

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24834

2、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。iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码（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-2018-24561、CNVD-2018-24562、CNVD-2018-24563、CNVD-2018-24567、CNVD-2018-245

68、CNVD-2018-24569、CNVD-2018-24570、CNVD-2018-24571）。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-2018-24561

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24562

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24563

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24567

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24568

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24569

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24570

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24571

3、Foxit 产品安全漏洞

Foxit Reader for Windows 是一款基于 Windows 平台的 PDF 文档阅读器。Foxit PhantomPDF for Windows 是它的商业版。本周，上述产品被披露存在内存错误引用漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 Foxit PhantomPDF for Windows 内存错误引用漏洞（CNVD-2018-24458、CNVD-2018-24459、CNVD-2018-24460、CNVD-2018-24461、CNVD-2018-24462、CNVD-2018-24463、CNVD-2018-24464）。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-2018-24458

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24459

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24460

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24461

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24462

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24463

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24464

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。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，造成拒绝服务。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2018-24474、CNVD-2018-24548、CNVD-2018-24552）、Linux kernel 无效指针解引用漏洞（CNVD-2018-24481、CNVD-2018-24480）、Linux kernel 空指针解引用漏洞（CNVD-2018-24483）、Linux kernel 拒绝服务漏洞（CNVD-2018-24547）、Linux kernel KVM virtualization 子系统权限提升漏洞。上述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-2018-24474

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24548

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24552

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24481

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24480

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24483

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24547

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24550

5、INVT Electric VT-Designer 堆缓冲区溢出漏洞

Electric VT-Designer 是一款图形开发工具。本周，INVT Electric VT-Designer 被披露存在堆缓冲区溢出漏洞。远程攻击者可利用该漏洞造成程序崩溃或执行代码。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-2018-24486

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-2018-24466	多款 RICOH Interactive Whiteboard 产品限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ricoh.com/info/2018/1127_1.html
CNVD-2018-24470	Zoom Client 信息欺骗漏洞	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://www.tenable.com/security/research/tra-2018-40
CNVD-2018-24489	Cisco Prime License Manager SQL 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181128-plm-sql-inject
CNVD-2018-24555	Http-signature 存在未明漏洞	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/joyent/node-http-signature/issues/10
CNVD-2018-24573	Nagios XI Snoopy 未授权远程命令执行漏洞	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://www.nagios.org/
CNVD-201	Artifex Software Ghostscript	高	厂商已发布了漏洞修复程序，请及时

8-24642	安全绕过漏洞		关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16863
CNVD-2018-24640	Red Hat PolicyKit 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gitlab.freedesktop.org/zbyszek/polkit/commit/fbaab32cb4ed9ed5f1e3eea6cd317d443aa427dc
CNVD-2018-24659	Adobe Flash Player 内存错误引用漏洞（CNVD-2018-24659）	高	用户可联系供应商获得补丁信息：https://www.adobe.com/
CNVD-2018-24664	Growl 命令执行漏洞	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/tj/node-growl/pull/61
CNVD-2018-24828	Microsoft Hyper-V 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：http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0965

小结：本周，IBM 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意命令或发起拒绝服务攻击（消耗内存资源）。此外，Apple、Foxit、Linux 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，执行任意代码，造成拒绝服务。另外，PbootCMS 被披露堆缓冲区溢出漏洞。远程攻击者可利用该漏洞造成程序崩溃或执行代码。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、Joomla Content Editor Com_JCE 组件信息泄露漏洞

验证描述

Joomla 是一套开源的内容管理系统(CMS)。

Joomla Content Editor Com_JCE 组件存在信息泄露漏洞。攻击者可利用漏洞获取数据库备份信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=31588

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-24660

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. Mozilla Firefox 包含一个存在了 11 年的“验证对话框”

Firefox 浏览器中存在一个可被攻击者利用的漏洞，并且其用来捕获恶意网站上的用户信息已有 11 年。这一问题自 2007 年 4 月就被首次报道，而到现在都未被修复。该漏洞利用只需要在源代码中嵌入一个恶意的 iframe，就可以实现在另一个域上发出 HTTP 身份验证请求，这导致 iframe 在恶意站点上显示身份验证模式。最新的示例来自于近日再次报告该问题的用户：登录框跳出后，其中一个正试图强迫他安装可疑 Firefox 扩展程序。恶意页面打开了浏览器的全屏模式，然后网页跳出了虚假的 Windows 对话框。因为这个登录对话框的原因，按 ESC 退出全屏或者点击选项卡中的窗口的关闭按钮都不起作用，点击登录对话框的关闭按钮或取消按钮，就会重新出现对话框，除非杀掉 Firefox 进程问题才会解决。

参考链接：https://www.cnbeta.com/articles/tech/796495.htm

2. D-Link DIR-850L 路由器存在漏洞，可绕过加密

D-Link DIR-850L 无线 AC 路由器（硬件修订版本 A）中存在漏洞。该漏洞使攻击者无需提供凭据即可完全访问无线网络。我们的方法在接入点连接期间跳过关键步骤，完全绕过加密。在确定此漏洞后，新思科技继续与芬兰国家网络安全中心（NCSC-FI）协调披露事宜，编号为 CVE-2018-18907。D-Link 已经为受影响的设备提供了修复方案。

参考链接：https://www.freebuf.com/vuls/190956.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