国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 11 月 26 日-2018 年 12 月 02 日 **2018 年第 48 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 213 个，其中高危漏洞 45 个、中危漏洞 159 个、低危漏洞 9 个。漏洞平均分值为 5.69。本周收录的漏洞中，涉及 0day 漏洞 66 个（占 31%），其中互联网上出现“Degrau Publicidade e Internet Plataforma de E-commerce SQL 注入漏洞、webERP Manufacturing 组件 SQL 注入漏洞”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 884 个，与上周（1352 个）环比下降 35%。

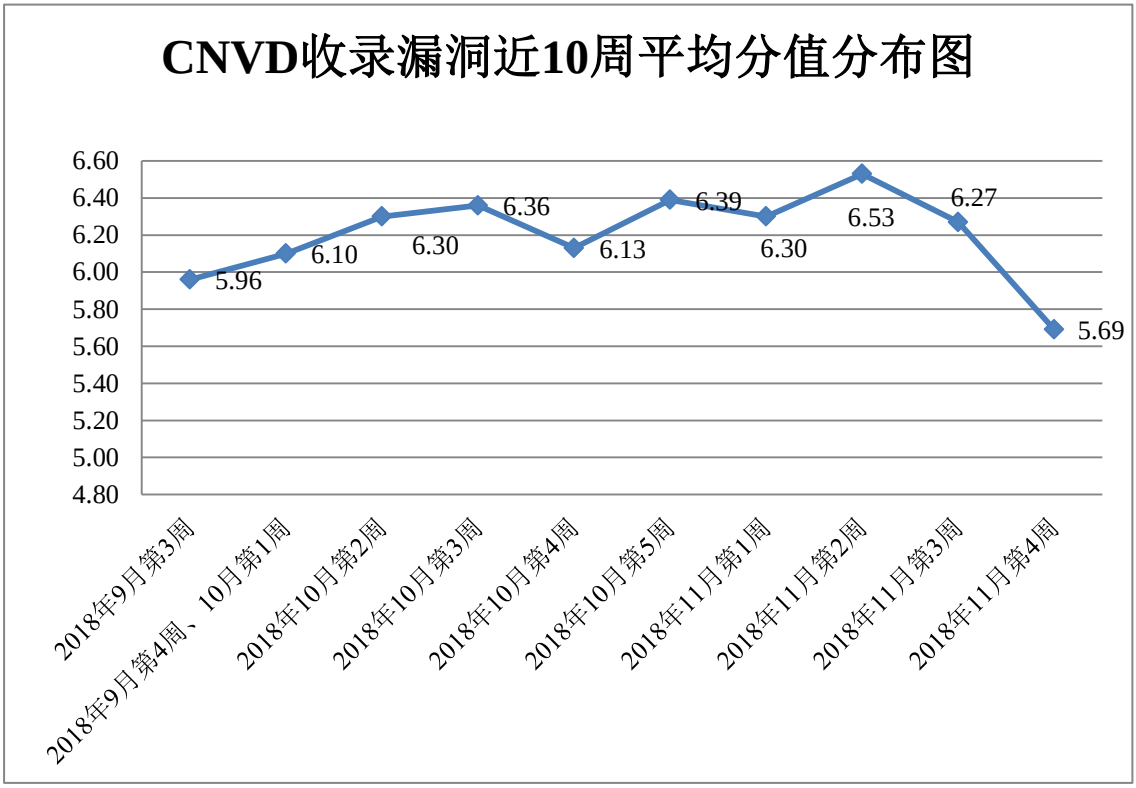

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 26 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 306 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 64 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：

网际傲游(北京)科技有限公司、广东百城人才网络股份有限公司、北京杰控科技有限公司、合肥汉思信息技术有限责任公司、济南杰飞软件有限公司、浙江易舸软件有限公司、漳州豆壳网络科技有限公司、嘉兴想天信息科技有限公司、北京联达动力信息科技发展有限公司、北京金山云网络技术有限公司、中山市商友网络科技有限公司、东莞市光速网络技术有限公司、梅州市青云客网络科技有限公司、珠海点典视觉设计有限公司、合众商道(大连)科技有限公司、智士软件(北京)有限公司、上海亿速网络科技有限公司、浙大恩特网络科技有限公司、长沙德尚网络科技有限公司、长沙翱云网络科技有限公司、苏州烟火网络科技有限公司、北京康盛新创科技有限责任公司、湖南梦行科技有限公司、淄博闪灵网络科技有限公司、济南泰创软件科技有限公司、中国海事仲裁委员会、易迅软件工作室、兔子影视、老班 CMS、LJCMS、Thinksaas、小二胡工作室、和利时集团、中环互联网、春杰工作室、亚马逊、雷风影视、Zzzcms、phpMyAdmin。

本周，CNVD 发布了《关于 PHPCMS 2008 存在代码注入漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4779

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、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。山东云天安全技术有限公司、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、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、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、内蒙古奥创科技有限公司、上海启疆信息科技有限公司、山石网科通信技术有限公司、北京信联科汇科技有限公司、上海银基信息安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 884 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）和漏洞盒子向 CNVD 共享的白帽子报送的 552 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）	322	322
漏洞盒子	230	230
华为技术有限公司	193	0
哈尔滨安天科技集团股份有限公司	192	0
北京天融信网络安全技术有限公司	145	18
新华三技术有限公司	143	0
北京启明星辰信息安全技术有限公司	104	5
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	48	0
北京神州绿盟科技有限公司	42	0
中国电信集团系统集成有限责任公司	29	0
深信服科技股份有限公司	18	0
北京知道创宇信息技术有限公司	14	8
四川无声信息技术有限公司	4	0
沈阳东软系统集成工程有限公司	1	1
山东云天安全技术有限公司	53	53
北京圣博润高新技术股份有限公司	23	23
广州竞远安全技术股份有限公司	17	17
中新网络信息安全股份有限公司	15	15
安徽锋刃信息科技有限公司	8	8

北京国舜科技股份有限公司	7	7
南京联成科技发展股份有限公司	7	7
内蒙古奥创科技有限公司	4	4
上海启疆信息科技有限公司	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
上海银基信息安全技术股份有限公司	1	1
CNCERT 湖南分中心	14	14
CNCERT 四川分中心	5	5
CNCERT 黑龙江分中心	4	4
CNCERT 上海分中心	4	4
CNCERT 重庆分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 云南分中心	1	1
个人	130	130
报送总计	1844	884

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 162 个，操作系统漏洞 20 个，WEB 应用漏洞 16 个，网络设备漏洞 11 个，数据库漏洞 4 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	162
操作系统漏洞	20
WEB 应用漏洞	16
网络设备漏洞	11
数据库漏洞	4

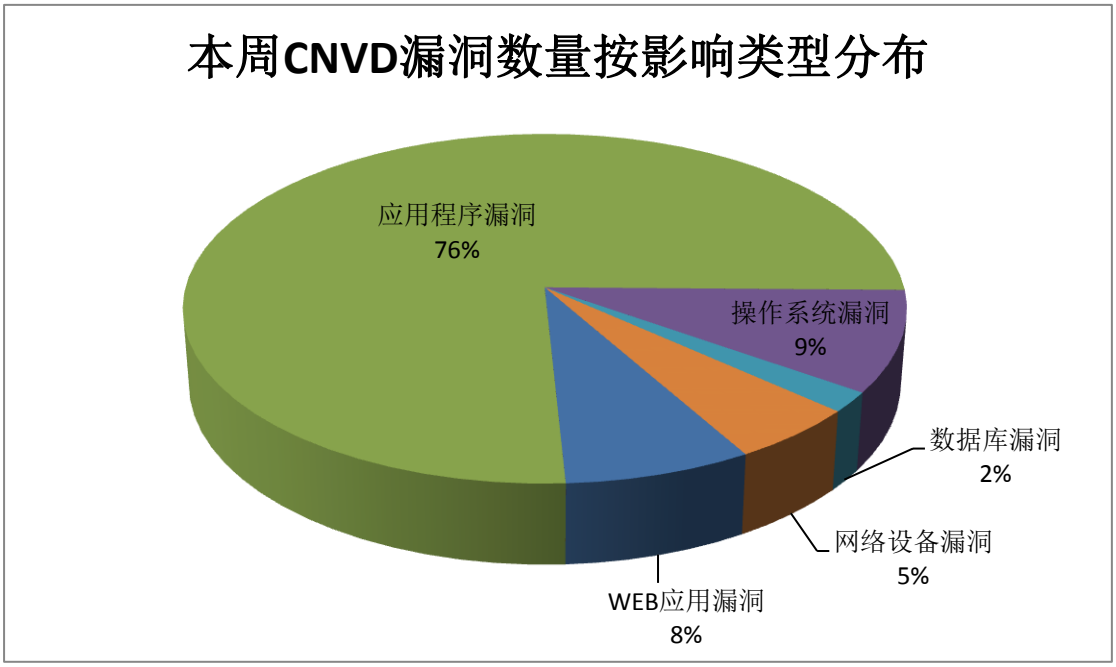

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、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	Oracle	73	34%
2	Google	15	7%
3	Linux	11	5%
4	IBM	9	4%
5	WordPress	7	4%
6	TIBCO	5	3%
7	TOTOLINK	5	3%
8	Artifex Software	3	1%
9	Microsoft	3	1%
10	其他	82	38%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，9 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“IBM DB2 db2pdcfg 缓冲区溢出漏洞、多款 Siemens 产品开放重定向漏洞 、Google Android Soc Infrastructure 缓冲区溢出漏洞、Oracle WebLogic

Server 存在未明漏洞（CNVD-2018-24321）”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/

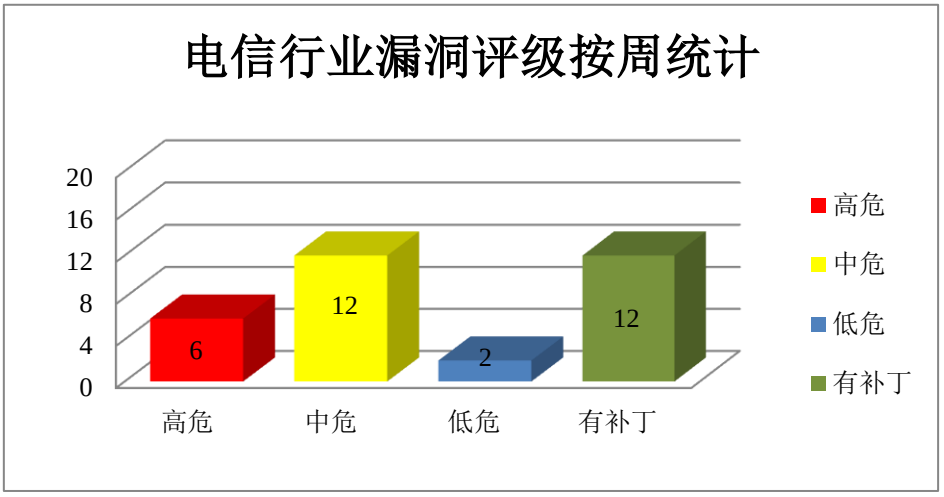

图 3 电信行业漏洞统计

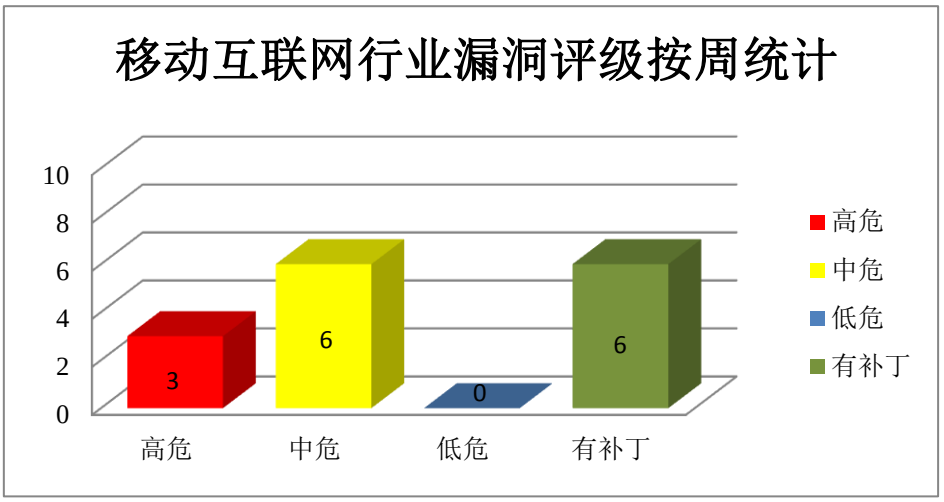

图 4 移动互联网行业漏洞统计

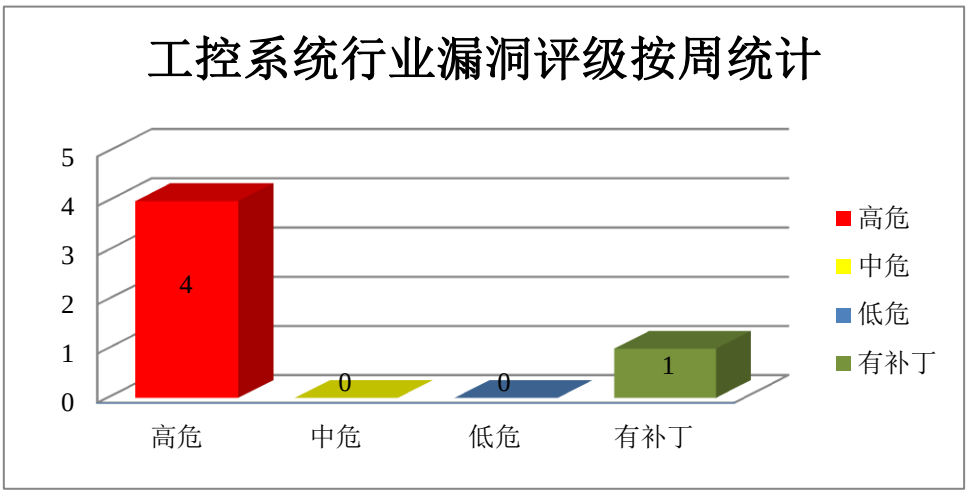

图 5 工控系统行业漏洞统计

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、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，攻击者可利用漏洞绕过沙盒，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Android Bootloader 缓冲区溢出漏洞、Google Android debugfs 模块缓冲区溢出漏洞、Google Android Soc Infrastructure 缓冲区溢出漏洞、Google Chrome PDFium 堆缓冲区溢出漏洞（CNVD-2018-24369）、Google Chrome ANGLE 内存破坏漏洞、Google Chrome V8 内存错引用漏洞、Google Chrome V8 远程代码执行漏洞、Google Chrome AppCache 沙盒绕过漏洞。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-2018-24295
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24301
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24299
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24369
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24372
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24373
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24375
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24376

2、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，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，提升权限，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 'mm/vmacache.c'本地权限提升漏洞、Linux Kernel 'fs/proc/base.c'本地信息泄露漏洞、Linux kernel 信息泄露漏洞（CNVD-2018-24296）、Linux kernel 越界访问漏洞、Linux kernel 内存错误引用漏洞（CNVD-2018-24386、CNVD-2018-24384、CNVD-2018-24387）、Linux kernel 越界访问漏洞（CNVD-2018-24385）。其中，“Linux kernel 内存错误引用漏洞（CNVD-2018-24384）、Linux kernel 越界访问漏洞（CNVD-2018-24385）”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-2018-24031

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24029

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24296

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24381

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24386

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24384

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24385

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24387

3、Oracle 产品安全漏洞

Oracle E-Business Suite 是在原来 Application（ERP）基础上的扩展，包括 ERP（企业资源计划管理）、HR（人力资源管理）、CRM（客户关系管理）等等多种管理软件的集合，是无缝集成的一个管理套件。Oracle FLEXCUBE Universal Banking 是一项实时、在线、全面的全球核心银行业务方案，涵盖零售、企业及投资银行业务。Oracle Banking Payments 是一个完整的支付处理解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响机密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle E-Business Suite 信息泄露漏洞、Oracle FLEXCUBE Universal Banking 信息泄露漏洞（CNVD-2018-24134）、Oracle FLEXCUBE Universal Banking 存在未明漏洞（CNVD-2018-24135、CNVD-2018-24136、CNVD-2018-24137）、Oracle FLEXCUBE Universal Banking 拒绝服务漏洞（CNVD-2018-24140）、Oracle Banking Payments 信息泄露漏洞（CNVD-2018-24143）、Oracle Banking Payments 拒绝服务漏洞。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-2018-24111

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24134

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24135

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24136

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24137

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24140

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24143

http://www.cnvd.org.cn/flaw/show/CNVD-2018-24149

4、IBM 产品安全漏洞

IBM Spectrum Protect（前称 Tivoli Storage Manager）是一套数据保护平台，它为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。IBM Spectrum Protect Client 是它的客户端程序。Spectrum Protect for Virtual Environments

是虚拟环境版本。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM WebSphere Portal 是一套企业门户软件。IBM Cloud 是一套开放式标准的云平台。WebSphere Application Server 是其中的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。IBM Rational Engineering Lifecycle Manager 是一套工程生命周期管理软件。IBM Rational Collaborative Lifecycle Management 是一套协作化生命周期管理解决方案。Rational Quality Manager（RQM）是一套协作的、基于 Web 的质量管理解决方案。Jazz Foundation 是其中的一个软件开发协作平台。IBM Spectrum Symphony 是一套用于在共享网格上运行计算和数据密集型分布式应用程序的企业级管理软件。IBM DB2 是一套关系型数据库管理系统。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，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：IBM Spectrum Protect Client 和 Spectrum Protect for Virtual Environments 拒绝服务漏洞、IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2018-24264）、IBM WebSphere Portal 跨站脚本漏洞（CNVD-2018-24362）、IBM WebSphere Application Server 信息泄露漏洞（CNVD-2018-24363）、IBM Rational Engineering Lifecycle Manager XML 外部实体注入漏洞（CNVD-2018-24366）、IBM Jazz Foundation 跨站脚本漏洞（CNVD-2018-24367）、IBM Spectrum Symphony 信息泄露漏洞、IBM DB2 db2pdcfg 缓冲区溢出漏洞。其中，“IBM Rational Engineering Lifecycle Manager XML 外部实体注入漏洞（CNVD-2018-24366）、IBM DB2 db2pdcfg 缓冲区溢出漏洞”的综合评级为“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-2018-24265
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24264
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24362
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24363
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24366
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24367
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24380
http://www.cnvd.org.cn/flaw/show/CNVD-2018-24388

5、PbootCMS 代码执行漏洞

PbootCMS 是一款使用 PHP 语言开发的开源企业建站内容管理系统（CMS）。本周，PbootCMS 被披露存在代码执行漏洞。远程攻击者可利用该漏洞执行代码。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-2018-24253

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-2018-24091	TIBCO Rendezvous 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://www.tibco.com/support/advisories/2018/11/tibco-security-advisory-november-6-2018-tibco-rendezvous
CNVD-2018-24092	Microsoft Excel 远程代码执行漏洞（CNVD-2018-24092）	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-2018-8577
CNVD-2018-24150	Apache Hadoop 任意文件写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://hadoop.apache.org/cve_list.html#cve-2018-8009-http-cve-mitre-org-cgi-bin-cvename-cgi-name-cve-2018-8009-zip-slip-impact-on-apache-hadoop
CNVD-2018-24157	NetApp SANtricity Web Services Proxy 和 SANtricity Storage Manager 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://security.netapp.com/advisory/ntap-20180612-0001/
CNVD-2018-24158	SUSE open build service 文件上传漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugzilla.suse.com/show_bug.cgi?id=736243
CNVD-2018-24176	TIBCO FTL realm server 组件跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tibco.com/support/advisories/2018/11/tibco-security-advisory-november-6-2018-tibco-ftl
CNVD-2018-24247	多款 Siemens 产品开放重定向漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.industry.siemens.com/cs/document/109755826/updates-for-step-7-v15-and-wincc-v15?dti=0&lc=en-WW
CNVD-2018-24270	PHP 内存错误引用漏洞（CNVD-2018-24270）	高	厂商已发布漏洞修复程序，请及时关注更新：https://bugs.php.net/patch-display.php?bug=76409&patch=avoid-double-free.pat

			ch&revision=1528027735
CNVD-2018-24305	Pivotal Operations Manager 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://pivotal.io/security/cve-2018-15762
CNVD-2018-24310	FreeBSD 缓冲区溢出漏洞（CNVD-2018-24310）	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.freebsd.org/security/advisories/FreeBSD-EN-18:13.icmp.asc

小结：本周，Google 被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒，执行任意代码或发起拒绝服务攻击。此外，Linux、Oracle、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，提升权限，执行任意代码，发起拒绝服务攻击等。另外，PbootCMS 被披露存在代码执行漏洞。远程攻击者可利用该漏洞执行代码。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、webERP Manufacturing 组件 SQL 注入漏洞

验证描述

webERP 是一套开源的进销存与财务管理系统（ERP 系统）。该系统支持库存管理、权限角色管理、订单管理和财务管理等。Manufacturing 是其中的一个组件。

webERP 4.15 版本中的 Manufacturing 组件的 CollectiveWorkOrderCost.php 文件存在 SQL 注入漏洞，远程攻击者可借助‘SearchParts’参数利用该漏洞获取企业 ERP 的敏感信息。

验证信息

POC 链接：https://github.com/0xUhaw/CVE-Bins/tree/master/webERP%20SQLI-2

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-24185

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. Windows VBScript 引擎远程执行代码漏洞(CVE-2018-8373)

VBScript 引擎处理内存中对象的方式中存在一个远程执行代码漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式来破坏内存。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后攻击者可以安装程序;查看，更改或删除数据;或创建具有完全用户权限的新帐户。

参考链接：https://www.freebuf.com/vuls/190601.html

2. 西门子警告，控制器平台中存在 Linux、GNU 错误

最近，西门子通知客户，其 SIMATIC S7-1500 工业自动化控制器的多功能平台中部分 Linux 与 GNU 组件受到 20 余个漏洞影响。据悉，西门子一年前宣布，将通过新多功能平台对 SIMATIC S7-1500 控制器产品组合进行扩展，允许工厂结合单个设备的控制与 PC 能力在控制器中运行多个应用程序。用户可以实时运行 C++应用程序，但该平台还允许特定客户轻松实现高级语言应用程序。西门子表示，为确保设备安全，将定期发布更新。

参考链接：https://www.easyaq.com/news/1701701661.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