国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 9 月 17 日-2018 年 9 月 23 日　　2018 年第 38 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 109 个、中危漏洞 247 个、低危漏洞 19 个。漏洞平均分值为 5.96。本周收录的漏洞中，涉及 0day 漏洞 122 个（占 33%），其中互联网上出现“Oracle VirtualBox Manager 'Name Attribute'拒绝服务漏洞、Western Digital My Cloud 身份验证绕过漏洞”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 588 个，与上周（1267 个）环比下降 54%。

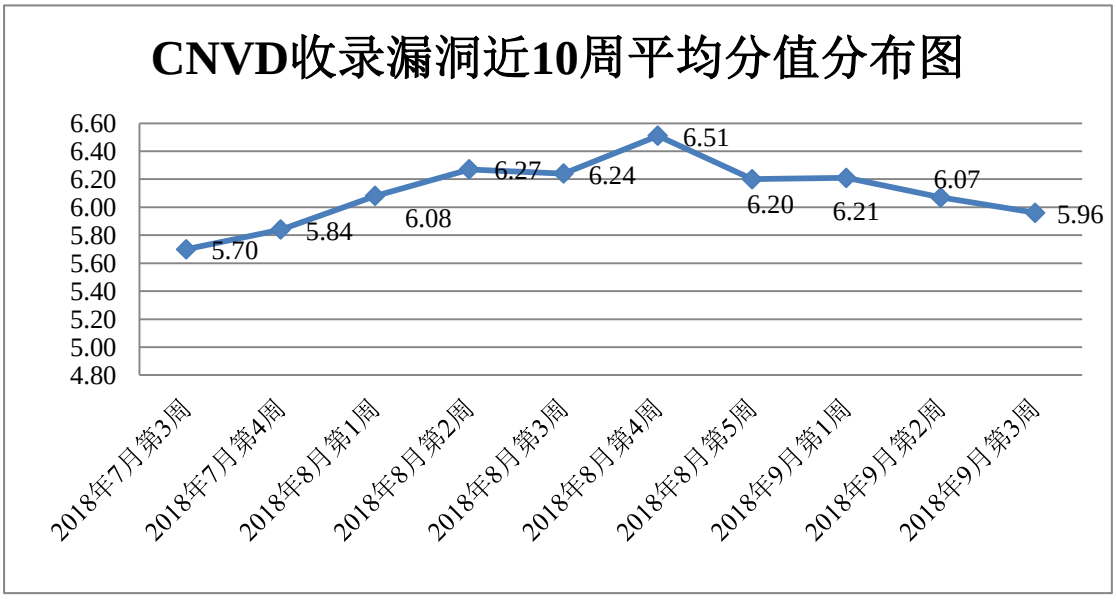

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 5 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 19 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 286 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 159 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 28 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：

金集团（香港）控股有限公司、北京江民新科技术有限公司、广州市卓杰计算机科技有限公司、二六三网络通信股份有限公司、北京科大天工科技服务有限公司、湖南梦行科技有限公司、北自所制造业自动化工程研究中心（常州）有限公司、中铁电气化铁路运营管理有限公司、上海鹏达计算机系统开发有限公司、长沙米拓信息技术有限公司、江西金磊科技发展有限公司、深圳市中威达物流有限公司、成都思乐科技有限公司、湖南建程信息科技有限公司、中国医药集团有限公司、正方软件股份有限公司、中科软科技股份有限公司、北京网宽天地科技有限公司、湖南翱云网络科技有限公司、无锡市速通运输有限公司、河南轩珩网络技术有限公司、上海卓卓网络科技有限公司、中国教育国际交流协会、中国工程师教育协会、中国钢铁产业科技服务综合平台、中华国际医学交流基金会、中国光伏农业网、中国建材工程资讯网、中国汽车信息网、安全牛网、畅梦网络、YCCMS、老班 CMS、SemCms。

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、哈尔滨安天科技股份有限公司、新华三技术有限公司、蓝盾信息安全技术有限公司、华为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、任子行网络技术股份有限公司、北京智游网安科技有限公司、中新网络信息安全股份有限公司、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、四川虹微技术有限公司（子午攻防实验室）、上海纽盾科技股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、海南神州希望网络有限公司、张家港款盾信息技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、河北盾安科技有限公司及其他个人白帽子向 CNVD 提交了 588 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 286 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
北京天融信网络安全技术有限公司	340	13
哈尔滨安天科技股份有限公司	202	0

360 网神（补天平台）	190	190
新华三技术有限公司	155	0
蓝盾信息安全技术有限公司	143	0
华为技术有限公司	130	0
中国电信集团系统集成有限责任公司	101	0
漏洞盒子	96	96
北京神州绿盟科技有限公司	94	0
北京数字观星科技有限公司	84	0
北京启明星辰信息安全技术有限公司	67	0
恒安嘉新(北京)科技股份公司	51	0
北京知道创宇信息技术有限公司	20	11
北京无声信息技术有限公司	15	5
深圳市深信服电子科技有限公司	11	0
厦门服云信息科技有限公司	8	1
山东云天安全技术有限公司	76	76
北京圣博润高新技术股份有限公司	47	47
任子行网络技术股份有限公司	23	23
北京智游网安科技有限公司	10	10
中新网络信息安全股份有限公司	10	10
南京联成科技发展股份有限公司	7	7
河南信安世纪科技有限公司	3	3
四川虹微技术有限公司（子午攻防实验室）	2	2

上海纽盾科技股份有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
海南神州希望网络有限公司	1	1
张家港欹盾信息技术有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
河北盾安科技有限公司	1	1
CNCERT 新疆分中心	4	4
CNCERT 山西分中心	3	3
CNCERT 广东分中心	1	1
CNCERT 安徽分中心	1	1
CNCERT 吉林分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 天津分中心	1	1
个人	76	76
报送总计	1979	588

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 204 个，WEB 应用漏洞 87 个，网络设备漏洞 39 个，操作系统漏洞 35 个，安全产品漏洞 10 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	204
WEB 应用漏洞	87
网络设备漏洞	39
操作系统漏洞	35
安全产品漏洞	10

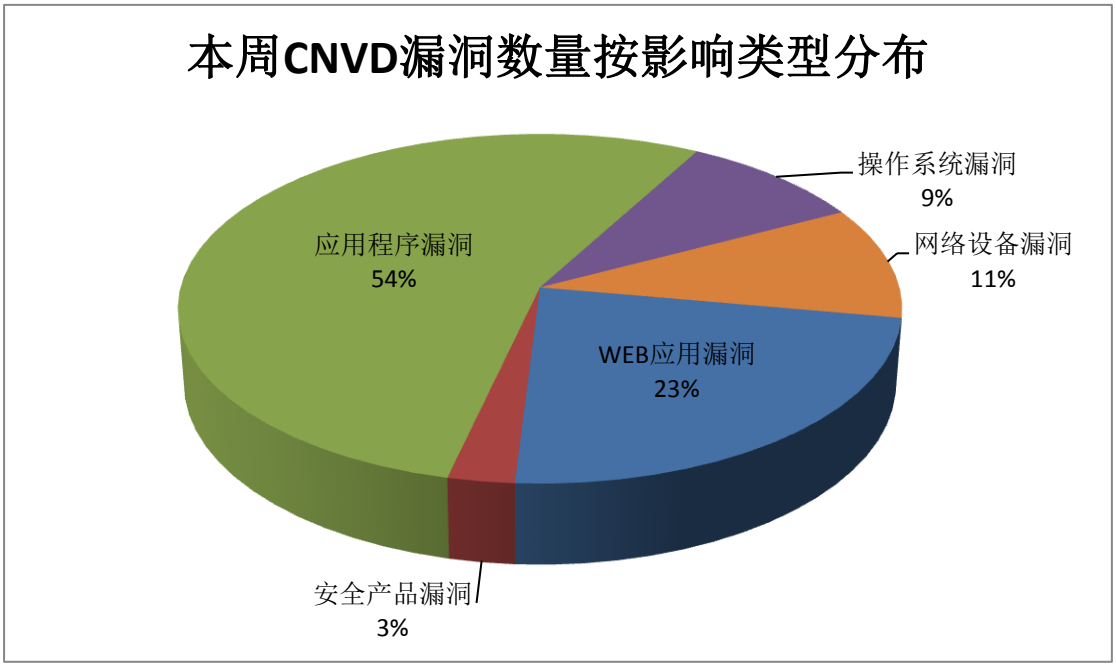

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Microsoft 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	27	7%
2	Google	22	6%
3	Microsoft	17	5%
4	Apache	16	4%
5	IBM	14	3%
6	Schneider Electric	7	2%
7	CloudBees	6	2%
8	HPE	6	2%
9	phpmywind	5	1%
10	其他	255	68%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，38 个移动互联网行业漏洞，24 个工控行业漏洞（如下图所示）。其中，“Google Android PMIC 缓冲区溢出漏洞、Fuji Electric V-Server 缓冲区溢出漏洞、Siemens SIMATIC STEP 7 和 WinCC 权限管理漏洞、Google

Android Qualcomm MProc 缓冲区溢出漏洞、Siemens SIMATIC STEP 7 和 WinCC 拒绝服务漏洞”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/

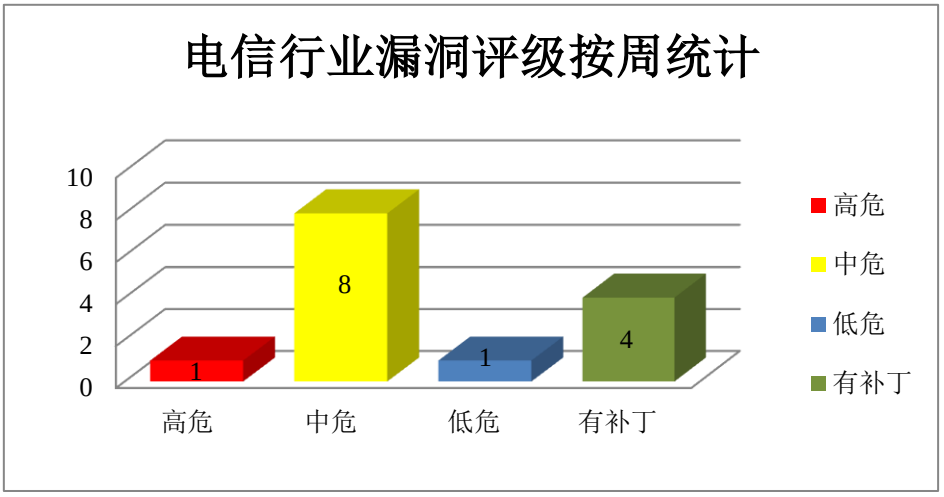

图 3 电信行业漏洞统计

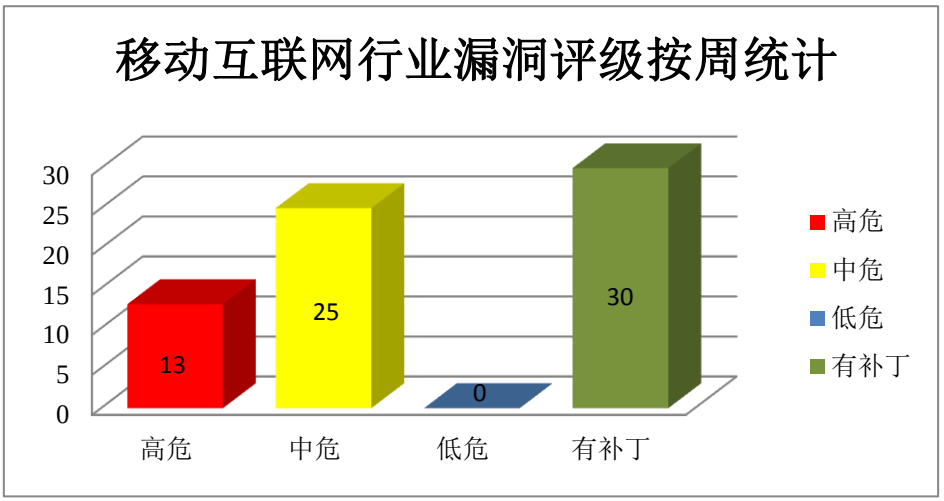

图 4 移动互联网行业漏洞统计

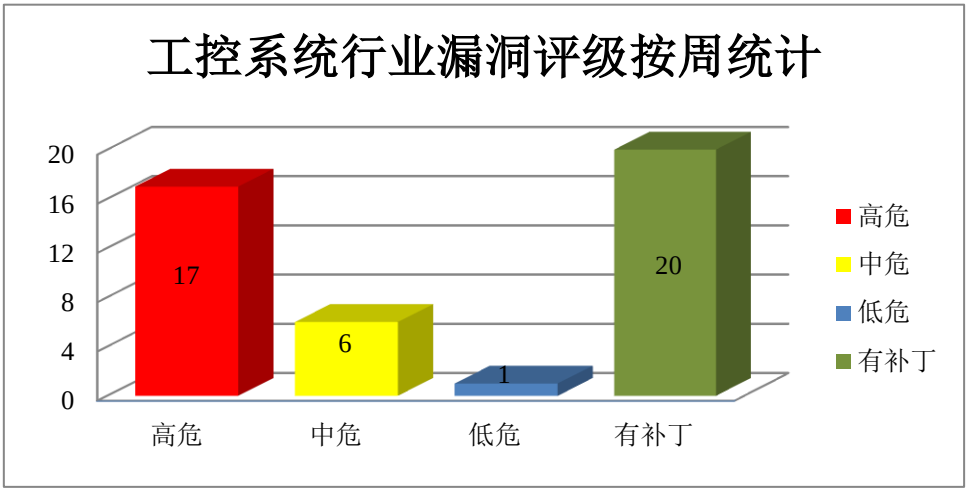

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows 7 SP1 是一套个人电脑使用的操作系统。Windows Server 2008 是一套服务器操作系统。Windows Server 2008 R2 SP1 是一套服务器使用的操作系统。Microsoft Windows 10 是一套供个人电脑使用的操作系统。Windows Server Version 1709 是一套服务器操作系统。Windows Server 2016 是一套服务器操作系统。Microsoft Internet Explorer 是一款流行的 WEB 浏览器。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，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Windows GDI+ Component 远程代码执行漏洞、Microsoft Windows Kernel 'Win32k.sys'本地权限提升漏洞（CNVD-2018-19388）、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2018-19391、CNVD-2018-19392、CNVD-2018-19393）、Microsoft Windows Kernel 'Win32k.sys'本地权限提升漏洞（CNVD-2018-19394）、Microsoft Windows NDIS 本地权限提升漏洞（CNVD-2018-19396）、Microsoft Windows Installer DLL 加载本地限提升漏洞。其中，除“Microsoft Windows Installer DLL 加载本地限提升漏洞”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-2018-19385

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19388

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19391

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19392

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19393

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19394

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19396

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19397

2、Apache 产品安全漏洞

Apache SpamAssassin 是的一款开源的垃圾邮件过滤器，它为系统管理员提供了一个过滤器，并支持对电子邮件进行分类阻止垃圾邮件。Apache Camel 是一套开源的基于 Enterprise Integration Pattern(企业整合模式，简称 EIP)的集成框架。Apache Traffic Server（ATS）是一款 HTTP 代理和缓存服务器。Apache Mesos 是一套支持 Hadoop、ElasticSearch 和 Spark 等应用架构的开源群集管理软件。Apache Cayenne 是一款提供对象关系映射（ORM）和远程服务的开源持久性框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞查看系统上的任意文件，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache SpamAssassin PDFInfo 插件远程代码执行漏洞、Apache Camel Mail 路径遍历漏洞、Apache Mesos libprocess 拒绝服务漏洞、Apache Cayenne CayenneModeler XML 外部实体注入漏洞、Apache Traffic Server 拒绝服务漏洞（CNVD-2018-19518、CNVD-2018-19519、CNVD-2018-19513、CNVD-2018-19517）。其中，“Apache SpamAssassin PDFInfo 插件远程代码执行漏洞、Apache Cayenne CayenneModeler XML 外部实体注入漏洞”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-2018-19407

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19409

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19511

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19520

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19518

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19519

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19513

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19517

3、Google 产品安全漏洞

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缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android Qualcomm MProc 缓冲区溢出漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-19554、CNVD-2018-19573、CNVD-2018-19572）、Google Android WLAN 缓冲区溢出漏洞（CNVD-2018-19576）、Google Android PMIC 缓冲区溢出漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-19581）、

Google Android Audio 缓冲区溢出漏洞。上述漏洞的综合评级为“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-2018-19405
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19554
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19573
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19572
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19576
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19575
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19581
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19583

4、IBM 产品安全漏洞

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。IBM Rational DOORS 是一套用于捕获、跟踪、分析和管理需求的软件。IBM FileNet Content Manager 和 Content Foundation 都是针对 FileNet P8 平台的内容管理解决方案。IBM Rational Quality Manager（RQM）是一套协作的、基于 Web 的质量管理解决方案。IBM Rational Collaborative Lifecycle Management（CLM）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。IBM Tivoli Monitoring（ITM）是一套系统监控软件。IBM GPFS 是一套专为 PB 级存储管理而优化的企业文件管理系统。IBM Spectrum Scale 是一套基于 IBM GPFS 的可扩展的数据及文件管理解决方案。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，提升权限，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 信息泄露漏洞（CNVD-2018-19104）、IBM Rational DOORS 权限提升漏洞、IBM FileNet Content Manager 和 Content Foundation Administration Console for Content Platform Engine XML 外部实体注入漏洞、IBM Rational Quality Manager 信息泄露漏洞、IBM Rational Quality Manager HTML 注入漏洞（CNVD-2018-19534）、多款 IBM 产品信息泄露漏洞（CNVD-2018-19536）、IBM Tivoli Monitoring 权限提升漏洞、IBM GPFS 拒绝服务漏洞。其中，“IBM Rational DOORS 权限提升漏洞、IBM Tivoli Monitoring 权限提升漏洞”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-2018-19104
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19527
http://www.cnvd.org.cn/flaw/show/CNVD-2018-19529

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19531

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19534

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19536

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19615

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19617

5、HPE 3PAR Service Processor 远程代码执行漏洞

HPE 3PAR Service Processor（SP）是一套部署在 VMware vSphere 虚拟机管理程序上的虚拟服务处理器。本周，HPE 3PAR Service Processor（SP）被披露存在远程代码执行漏洞。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-2018-19548

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-2018-19045	DisplayLink Core Software Cleaner Application 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.displaylink.com/downloads/windows
CNVD-2018-19102	QNAP QTS Music Station 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.qnap.com/zh-tw/security-advisory/nas-201809-14
CNVD-2018-19281	Dell EMC Unity 验证绕过漏洞	高	用户可联系供应商获得补丁信息：https://support.emc.com/downloads/39949_Dell-EMC-Unity-Family
CNVD-2018-19399	Cisco Webex Network Recording Player 远程代码执行漏洞（CNVD-2018-19399）	高	思科发布了解决上述漏洞的软件更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180919-webex
CNVD-2018-19413	Pivotal Application Service Pivotal Applications Manager 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://pivotal.io/security/cve-2018-11088
CNVD-2018-19414	Cloud Foundry Container Runtime 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.cloudfoundry.org/blog/cve-2018-1223/
CNVD-2018-19423	Puppet Enterprise 明文传输漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://puppet.com/security/cve/cve-2018-11749
CNVD-2018-19547	Moodle 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://moodle.org/mod/forum/discuss.php?d=376023
CNVD-2018-19553	Linksys Velop 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.linksys.com/us/support-article?articleNum=207568
CNVD-2018-19589	多款华为产品信息泄露漏洞	高	华为已发布版本修复该漏洞，安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20180919-02-smartphone-cn

小结：本周，Microsoft 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，破坏内存。此外，Apache、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，提升权限，执行任意代码，发起拒绝服务攻击等。另外，HPE 3PAR Service Processor（SP）被披露存在远程代码执行漏洞。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、Oracle VirtualBox Manager 'Name Attribute'拒绝服务漏洞

验证描述

Oracle VirtualBox Manager 是 Oracle 公司推出的虚拟化管理工具。

Oracle VirtualBox Manager 'Name Attribute'存在拒绝服务漏洞，攻击者可利用漏洞造成系统崩溃。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=30904

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-19064

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. Windows 任务计划程序被曝存在 0 day 漏洞

近期，研究人员在 Windows 任务计划程序的一个 API 中发现了一个安全漏洞，该漏洞存在于 Windows 10 和 Windows Server 2016 64 位操作系统任务计划程序的高级本地程序调用（ALPC）接口之中，这两个版本的操作系统中 ALPC 的 API 函数未对请求权限进行正确的验证，因此任何本地攻击者都将可以对请求数据进行修改，实现提权。

参考链接：http://www.freebuf.com/news/183952.html

2. 西数 NAS 出现严重安全漏洞，攻击者可获得完整访问权限

西部数据（Western Digital）广受欢迎的 My Cloud 系列网络附加存储（NAS）设备，近日曝出了一个严重的安全漏洞，导致攻击者可以完全访问设备里的内容。荷兰安全研究员指出：身份验证绕过漏洞允许攻击者在登录设备之前获得管理员权限，他们只需创建反向 shell，便可访问驱动器上的用户文件。

参考链接：https://www.cnbeta.com/articles/tech/769825.htm

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