国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 05 月 16 日-2016 年 05 月 22 日　　2016 年第 21 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 219 个，其中高危漏洞 83 个、中危漏洞 123 个、低危漏洞 13 个。漏洞平均分值为 6.26 分。本周收录的漏洞中，涉及 0day 漏洞 5 个（占 2%）。其中互联网上出现“eXtplorer 目录遍历漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。此外，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 1064 个，与上周（1185 个）环比下降 10%。

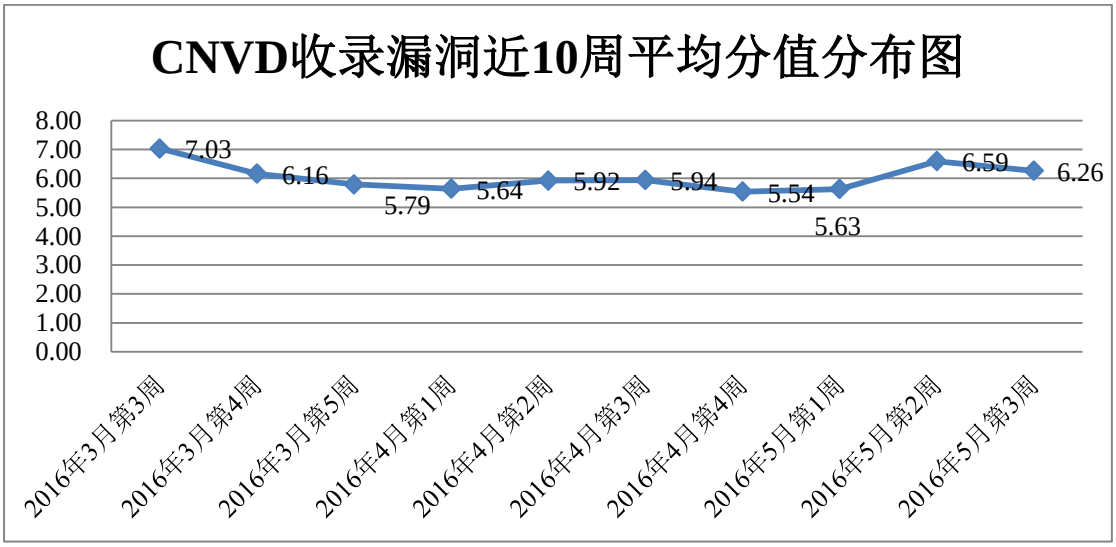

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及个人报送了本周收录的全部 219 个漏洞。报送情况如表 1 所示。其中，启明星辰、东软、安天实验室等单位报送数量较多。补天平台、乌云、漏洞盒子、深圳市深信服电子科技有限公司、福建六壬网安股份有限公司及白

帽子向 CNVD 提交了 1064 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎(补天平台)	578	578
乌云	433	433
启明星辰	189	0
东软	193	0
安天实验室	160	0
杭州安恒信息技术有限公司	99	0
天融信	96	0
恒安嘉新	77	2
绿盟科技	70	0
中国电信集团系统集成有限责任公司	47	2
漏洞盒子	27	27
H3C	8	0
深圳市深信服电子科技有限公司	6	6
福建六壬网安股份有限公司	1	1
个人	15	15
报送总计	1999	1064
录入总计	219（去重）	1064

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 219 个漏洞。其中应用程序漏洞 166 个，Web 应用漏洞 24 个，操作系统漏洞 14 个，网络设备漏洞 8 个，安全产品漏洞 6 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量

应用程序漏洞	166
web 应用漏洞	24
操作系统漏洞	14
网络设备漏洞	8
安全产品漏洞	6
数据库漏洞	1

表 2 漏洞按影响类型统计表

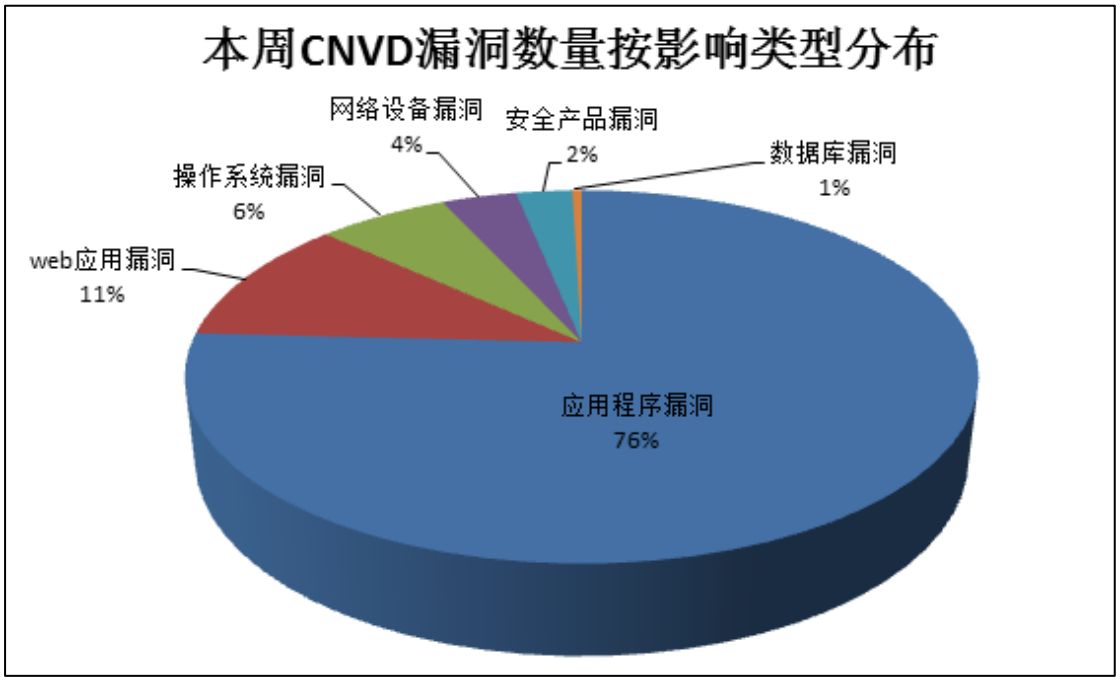

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、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。

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	71	32%
2	IBM	12	5%
3	Cisco	11	5%
4	Linux	9	4%
5	Moodle	5	2%
6	Apple	5	2%
7	Google	5	2%
8	Red Hat	4	2%
9	Siemens	2	1%
10	其他	95	45%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，2 个移动互联网行业漏洞，8 个工控系统行业漏洞（如下图所示）。其中，“Huawei 3G/LTE 本地提权漏洞、Apple iOS WebKit Canvas 任意代码执行漏洞、Meteocontrol WEB'log 任意命令执行漏洞”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/

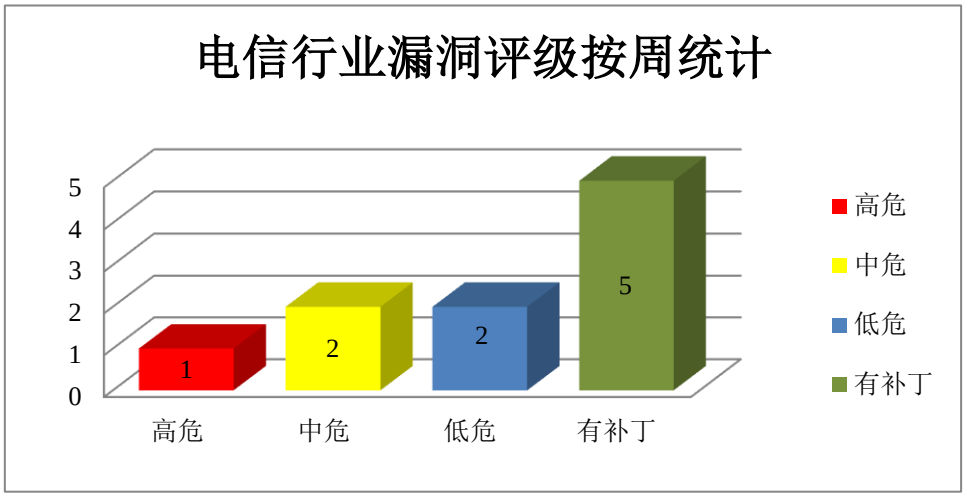

图 3 电信行业漏洞统计

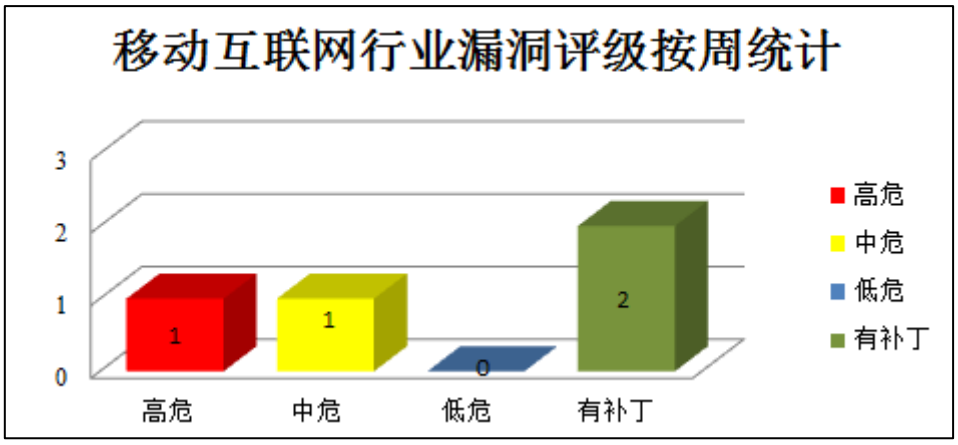

图 4 移动互联网行业漏洞统计

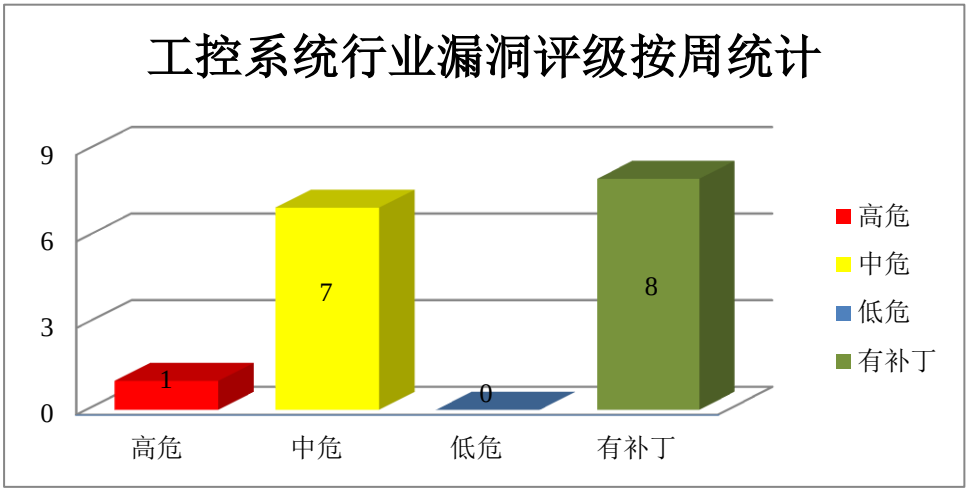

图 5 工控系统行业漏洞统计

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 DC 等都是美国奥多比（Adobe）公司的产品。Acrobat DC 是一套桌面版 PDF 解决方案；Acrobat Reader DC 是一套用于查看、打印和批注 PDF 的工具。Classic 和 Continuous 是 Acrobat DC 和 Acrobat Reader DC 产品下载中心所提供的两种更新机制。Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。本周，上述产品被披露存在内存破坏漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品内存破坏漏洞（CNVD-2016-03144、CNVD-2016-03145、CNVD-2016-03146、CNVD-2016-03147、CNVD-2016-03148、CNVD-2016-03149、CNVD-2016-03152、CNVD-2016-03153）等。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-2016-03144

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03145

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03146

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03147

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03148

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03149

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03152

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03153

2、Cisco 产品安全漏洞

Cisco Web Security Appliance（WSA）是美国思科（Cisco）公司的一套 Web 安全设备。该设备提供基于 SaaS 的访问控制、实时网络报告和追踪、制定安全策略等功能。Cisco Adaptive Security Appliance（ASA，自适应安全设备）是美国思科（Cisco）公司的一套防火墙设备。Cisco Unified Computing System（UCS）Central 是美国思科（Cisco）公司的一套对 Cisco UCS 服务器域进行管理的软件。Cisco IOS on Industrial Ethernet（IE）4000 和 Industrial Ethernet（IE）5000 是美国思科（Cisco）公司的一套运行于 Cisco IE 4000 和 5000 系列交换机产品中的操作系统。Cisco Cloud Network Automation Provisioner 是一套云网络自动化配置软件。本周，上述产品被披露存在跨站脚本、SQL 注入和拒绝服务漏洞，攻击者利用漏洞可注入任意 Web 脚本或 HTML，获取数据库数据和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Web Security Appliance AsyncOS 拒绝服务漏洞、Cisco Web Security Appliance AsyncOS 拒绝服务漏洞（CNVD-2016-03366、CNVD-2016-03367、CNVD-2016-03368）、Cisco Adaptive Security Appliance Ipsec 代码拒绝服务漏洞、Cisco Unified Computing System Central 跨站脚本漏洞、Cisco Cloud Network Automation Provisioner SQL 注入漏洞、Cisco Industrial Ethernet 4000 和 Ethernet 5000 IOS 拒绝服务漏洞等。其中，“Cisco Web Security Appliance AsyncOS 拒绝服务漏洞、Cisco Web Security Appliance AsyncOS 拒绝服务漏洞（CNVD-2016-03366、CNVD-2016-03367、CNVD-2016-03368）”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-2016-03366
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03367
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03368
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03369
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03360
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03359
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03207
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03253

3、 IBM 产品安全漏洞

IBM Marketing Platform 是美国 IBM 公司的一套营销平台。IBM Emptoris Sourcing 是美国 IBM 公司的一套寻源到合同解决方案。IBM Cognos TM1 是美国 IBM 公司的一套用于规划、预算编制、预测和分析的企业规划软件。IBM Rational Collaborative Lifecycle Management（CLM）等都是美国 IBM 公司的产品。IBM Rational CLM、Rational Team Concert（RTC）和 Rational Engineering Lifecycle Manager 都是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；Rational Requirements Composer 和 Rational DOORS Next Generation 都是需求管理解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者利用上述漏洞可执行任意 SQL 命令、注入任意 Web 脚本或 HTML、泄露敏感信息和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM Marketing Platform SQL 注入漏洞、IBM Marketing Platform SQL 注入漏洞（CNVD-2016-03333）、IBM Marketing Platform 跨站脚本漏洞、IBM Emptoris Sourcing 开放重定向漏洞、IBM Cognos TM1 拒绝服务漏洞、多款 IBM Rational 产品跨站脚本漏洞、多款 IBM Rational 产品权限获取漏洞、IBM Rational Team Concert HTML 注入漏洞等。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-2016-03333

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03334

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03335

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03343

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03256

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03210

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03209

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03206

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，上述产品被披露存在安全绕过、信息泄露、内存错误引用和拒绝服务漏洞，允许攻击者利用漏洞绕过安全限制、泄露敏感信息、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 信息泄露漏洞（CNVD-2016-03218、CNVD-2016-03352）、 Linux kernel 拒绝服务漏洞（CNVD-2016-03217、CNVD-2016-03194、CNVD-2016-03199）、Linux kernel 内存错误引用漏洞（CNVD-2016-03350）、Linux kernel BPF 拒绝服务漏洞、Linux kernel 安全绕过漏洞（CNVD-2016-03201）等。其中，“Linux kernel 信息泄露漏洞（CNVD-2016-03352）、Linux kernel 内存错误引用漏洞（CNVD-2016-03350）”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-2016-03218

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03352

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03217

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03194

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03199

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03350

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03200

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03201

5、eXtplorer 目录遍历漏洞

eXtplorer 是一套基于 PHP 的在线文件管理程序，它支持在线浏览文件和文件夹以及作为 FTP 客户端登录 FTP 服务器。本周，eXtplorer 被披露存在目录遍历漏洞，攻击者可借助包含‘../’字符的存档内容利用该漏洞覆盖任意文件。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序。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-2016-03355

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

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2016-03191	OpenJPEG 'opj_j2k_write_mco'函数内存错误引用漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/uclouvain/openjpeg/commit/940100c28ae28931722290794889cf84a92c5f6f
CNVD-2016-03205	Red Hat OpenShift Enterprise 权限提升漏洞	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://access.redhat.com/errata/RHSA-2016:1064
CNVD-2016-03197	Docker 权限获取漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.docker.com/
CNVD-2016-03196	Meteocontrol WEB'log 任意命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://us.meteocontrol.com/
CNVD-2016-03237	Symphony CMS SQL 注入漏洞	高	用户可联系供应商获得补丁信息：http://www.getsymphony.com/
CNVD-2016-03249	SAP NetWeaver Application Server Invoker Servlet 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://go.sap.com/
CNVD-2016-03250	ubuntu-core-launcher 程序包信息泄露漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.ubuntu.com/usn/USN-2956-1
CNVD-2016-03251	Botan 堆缓冲区溢出漏洞（CNVD-2016-03251）	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://botan.randombit.net/security.ht

			ml
CNVD-2016-03263	Tiny Tiny RSS SQL 注入漏洞	高	用户可联系供应商获得补丁信息：http://tiny-tiny-rss/backend.php
CNVD-2016-03252	Apple FileMaker 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://help.filemaker.com/app/answers/detail/a_id/15364

表 4 部分重要高危漏洞列表

小结：本周 Adobe 产品被披露存在内存破坏漏洞，攻击者利用漏洞可执行任意代码。此外，Cisco、IBM、Linux 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞注入任意 Web 脚本或 HTML、泄露敏感信息、执行任意代码和发起拒绝服务攻击等。另外，eXtplorer 被披露存在目录遍历漏洞，攻击者可借助包含‘../’字符的存档内容利用该漏洞覆盖任意文件。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。

本周漏洞要闻速递

1.漏洞预警：Docker Swarm Manager 远程管理端口访问

Docker 是一款国内外云平台常用的应用程序轻量级容器，AWS，百度等都有使用。通常用于轻量化部署应用。在 Docker Swarm 的部署文档中，由于默认存在某些不安全的配置样例，导致 Manager 的 2375 管理端口对外，可以造成写文件并通过写入 ssh key 文件获取系统 root 权限。其影响范围为：1、目前还在使用的所有版本的 Docker 2、所有使用 Docker swarm 的企业 3、可能影响对 Docker 默认配置进行修改的企业。

参考链接：http://www.freebuf.com/vuls/104666.html

2. 赛门铁克/诺顿反病毒引擎远程 Heap/Pool 内存损坏漏洞

近日，Symantec 和 Norton 产品中使用的核心杀毒引擎被曝存在高危漏洞。它在解析用 aspack 早期版本打包的可执行文件时会发生缓冲溢出，导致内存损坏，Windows 系统蓝屏。其 CVE 编号为 CVE-2016-2208。

参考链接：http://www.freebuf.com/vuls/104852.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：010-82990999