

信息安全漏洞周报

2016 年 03 月 21 日-2016 年 03 月 27 日

2016年第13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 115 个，其中高危漏洞 30 个、中危漏洞 79 个、低危漏洞 6 个。漏洞平均分为 6.16 分。本周收录的漏洞中，涉及 0day 漏洞 7 个（占 6%）。其中互联网上出现“GonafishLinksCaffe 身份验证绕过漏洞”零日代码攻击漏洞，请使用相关产品的用户注意加强防范。本周，互联网上披露了“Linux Kernel 'fs/pipe.c'存在多个本地内存破坏漏洞”，CNVD 提醒用户及时下载补丁更新。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 554 个，与上周（906 个）环比下降 39%。

CNVD收录漏洞近10周平均分分布图

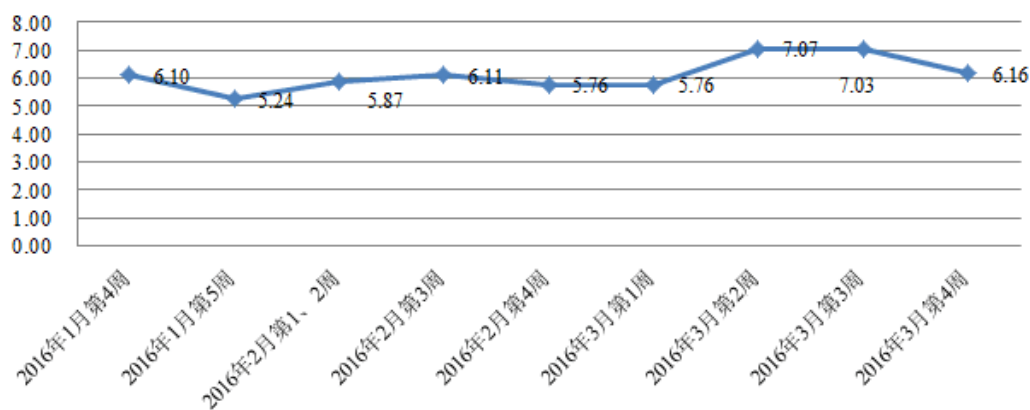


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 115 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、恒安嘉新、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子、腾讯玄武实验室、北京国舜科技股份有限公司、河

北翎贺计算机信息技术有限公司及白帽子向 CNVD 提交了 554 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
启明星辰	106	0
安天实验室	103	0
恒安嘉新	93	0
绿盟科技	92	0
奇虎(补天平台)	36	36
天融信	25	0
H3C	22	0
东软	10	0
乌云	471	471
漏洞盒子	18	18
腾讯玄武实验室	2	2
北京国舜科技股份有限公司	2	2
河北翎贺计算机信息技术有限公司	1	1
个人	24	24
报送总计	1005	554
录入总计	115（去重）	554

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 115 个漏洞。其中应用程序漏洞 48 个，网络设备漏洞 2 个，操作系统漏洞 44 个，Web 应用漏洞 18 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	48

操作系统漏洞	44
Web 应用漏洞	18
安全产品漏洞	3
网络设备漏洞	2

表 2 漏洞按影响类型统计表

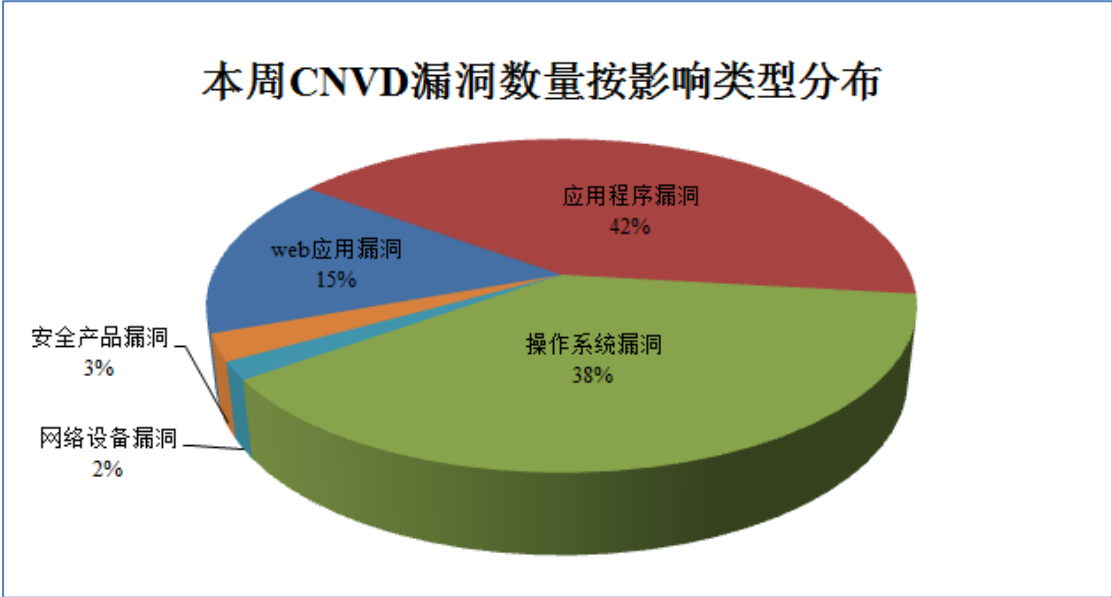


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Foxit、Moodle 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	Apple	46	40%
2	Foxit	10	9%
3	Moodle	10	9%
4	HP	8	7%
5	IBM	4	3%
6	Symantec	4	3%
7	Drupal	2	2%
8	Git	2	2%
9	Linux	2	2%
10	其他	27	23%

表 3 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 1 个电信行业漏洞、22 个移动互联网漏洞、2 个工控系统行业漏洞（如下图所示）。其中，“多款 Apple 产品 kernel 内存破坏漏洞、多款 Apple 产品 kernel 拒绝服务漏洞、多款 Apple 产品 kernel 任意代码执行漏洞、多款 Apple 产品 libxml 2 内存破坏漏洞、Apple iOS Kernel 内存破坏漏洞、Apple iOS IOHIDFamily 内存破坏漏洞、Apple iOS FontParser 内存破坏漏洞、Apple iOS AppleUSBNetworking 内存破坏漏洞、Apple iOS WebKit 内存破坏漏洞（CNVD-2016-01845）”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/>

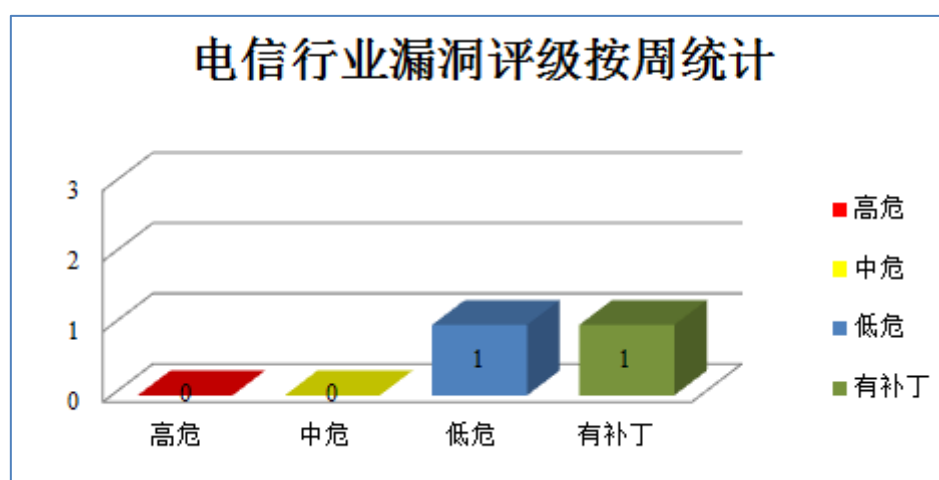


图 3 电信行业漏洞统计

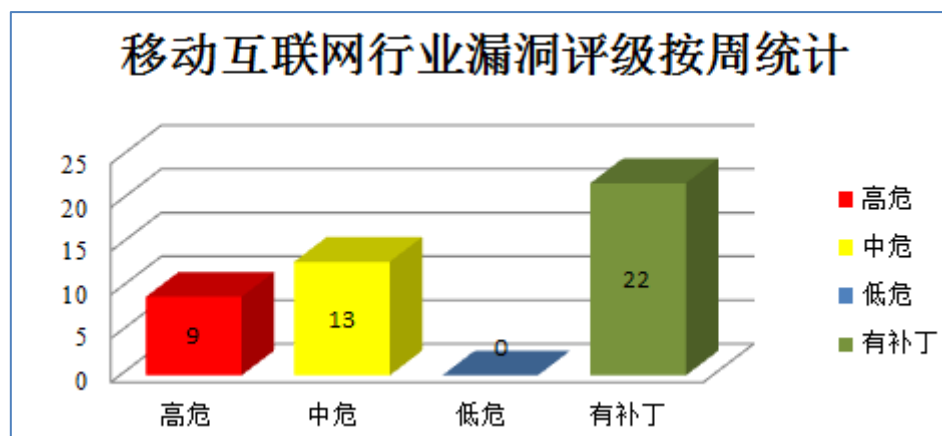


图 4 移动互联网行业漏洞统计

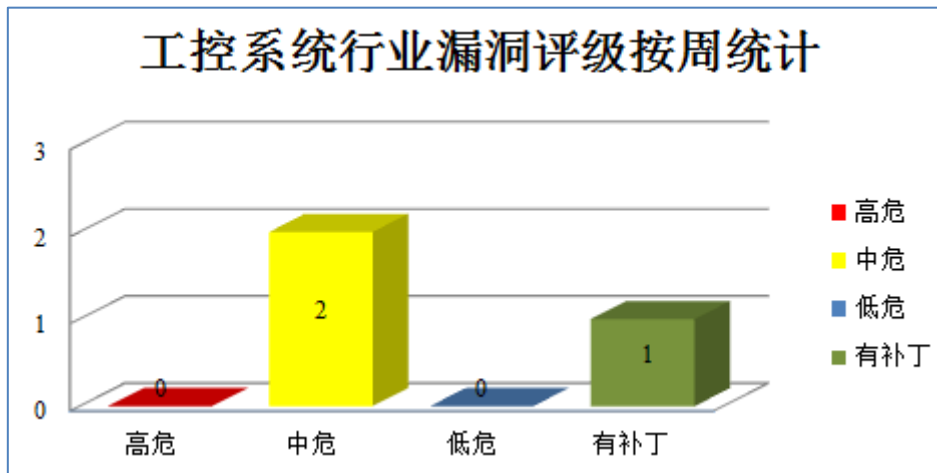


图 5 工控系统行业漏洞统计



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、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，该产品被披露存在内存泄露和内存破坏漏洞，远程攻击者可利用漏洞泄露内核内存、造成系统崩溃或提升系统权限。

CNVD 收录的相关漏洞包括：Linux kernel 内存泄露漏洞、Linux Kernel 'fs/pipe.c' 存在多个本地内存破坏漏洞。其中，“Linux Kernel 'fs/pipe.c' 存在多个本地内存破坏漏洞”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-2016-01836>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01828>

2、Apple 产品安全漏洞

Apple iOS、OS X、tvOS 和 watchOS 都是美国苹果（Apple）公司的产品。Apple iOS 是为移动设备所开发的一套操作系统；OS X 是为 Mac 计算机所开发的一套专用操作系统；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。kernel 是其中的一个内核组件。本周，上述产品被披露存在内存破坏、拒绝服务和远程代码执行漏洞等，远程攻击者可利用漏洞执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apple OS X kernel 内存破坏漏洞、多款 Apple 产品 kernel 内存破坏漏洞、多款 Apple 产品 kernel 拒绝服务漏洞、多款 Apple 产品 kernel 任意代码执行漏洞、Apple OS X NVIDIA Graphics Drivers 内存破坏漏洞、Apple OS X dyld 任意代码执行漏洞、Apple OS X Carbon 内存破坏漏洞、Apple OS X AppleRAI

D 组件内存破坏漏洞等。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-2016-01868>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01867>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01865>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01876>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01880>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01877>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01872>

3、Moodle 产品安全漏洞

Moodle 是澳大利亚马丁·多基马（Martin Dougiamas）博士开发的一套免费、开源的电子学习软件平台，也称课程管理系统、学习管理系统或虚拟学习环境。本周，该产品被披露存在设计漏洞、跨站脚本和跨站请求伪造漏洞等，远程攻击者可利用漏洞进行跨站脚本和跨站请求伪造攻击等。

CNVD 收录的相关漏洞包括：Moodle 'mod_assign_save_submission'函数设计漏洞、Moodle Assignment 插件跨站请求伪造漏洞、Moodle 'get_calendar_events'函数设计漏洞、Moodle Single View 设计漏洞、Moodle Event Monitor 设计漏洞、Moodle mod_data 高级搜索跨站脚本漏洞、Moodle 设计漏洞（CNVD-2016-01812、CNVD-2016-01813）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-2016-01805>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01806>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01807>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01808>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01809>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01810>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01812>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01813>

4、Foxit 产品安全漏洞

Foxit Reader 是一款小型的 PDF 文档查看器和打印程序。PhantomPDF 是通用的 PDF 编辑器。本周，上述产品被披露存在信息泄露和远程代码执行漏洞，攻击者利用漏洞可获取敏感信息和执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PhantomPDF Signature 字段内存错误引用远程

代码执行漏洞、Foxit Reader 修订号内存错误引用远程代码执行漏洞、Foxit Reader Format 操作内存错误引用远程代码执行漏洞、Foxit Reader XFA preOpen 内存错误引用远程代码执行漏洞、Foxit Reader XFA Page prePrint 事件内存错误引用远程代码执行漏洞、Foxit PhantomPDFListBox 值内存错误引用远程代码执行漏洞、Foxit Reader ConvertTo PDF JPEG 越界读信息泄露漏洞、Foxit Reader ConvertToPDF GIF 解析越界读信息泄露漏洞。目前，厂商已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-2016-01856>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01857>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01858>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01855>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01854>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01852>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01851>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01850>

5、IBM Tivoli NetView Access Services 权限获取漏洞

IBM Tivoli NetView Access Services (NVAS) 是美国 IBM 公司的一套支持从一个终端同时访问多个应用程序的会话管理工具。本周，IBM Tivoli NetView Access Services (NVAS) 被披露存在权限获取漏洞，攻击者可利用漏洞获取权限。目前，厂商尚未发布漏洞修补程序。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-2016-01758>

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-2016-01739	HP System Management Homepage 权限控制漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c05045763
CNVD-2016-01747	Symantec Endpoint Protection Manager 和 Client 跨站脚本漏洞	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.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvaid=security_advisory&year=&suid=20160317_00
CNVD-2016-01746	Symantec Endpoint Protection Manager 和 Client SQL 注入漏洞	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.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160317_00
CNVD-2016-01745	Symantec Endpoint Protection Manager 和 Client 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160317_00
CNVD-2016-01751	PCRE 和 PCRE2 ‘compile_branch’ 函数拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://vcs.pcre.org/pcre/code/trunk/ChangeLog?view=markup&pathrev=1631
CNVD-2016-01750	SolarwindsDameware Remote Mini Controller dwmrccs 守护进程缓冲区溢出漏洞	高	暂无
CNVD-2016-01769	OpenSSHxauth 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.openssh.com/txt/x11fwd.adv
CNVD-2016-01765	iTop 远程代码执行漏洞	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://sourceforge.net/p/itop/tickets/1202/
CNVD-2016-01767	Websitebaker SQL 注入漏洞（CNVD-2016-01767）	高	WebsiteBaker 2.8.3 SP6 RC3.0 已修复此漏洞，建议用户下载使用： http://addon.websitebaker.org/pages/en/browse-add-ons.php?id=06C9F242
CNVD-2016-01799	HP Operations Orchestration 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： https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05050545

表 4 部分重要高危漏洞列表

小结：本周，Linux 产品被披露存在内存泄露和内存破坏漏洞，远程攻击者可利用漏洞泄露内核内存、造成系统崩溃或提升系统权限。此外，Apple、Moodle、Foxit 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、进行跨站脚本和跨站请求伪造攻击、执行任意代码和发起拒绝服务攻击等。另外，IBM Tivoli NetView Access Services（NVAS）被披露存在一个高危漏洞，攻击者可利用漏洞获取权限。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. Oracle 发布紧急 Java 更新，修复关键漏洞

日前，Oracle 发布了紧急 Java 安全更新，修复了一个关键漏洞（CVE-2016-0636，CNNVD-201603-377）。Oracle 之所以如此迅速地做出回应，是因为该漏洞能轻易被利用，并且该漏洞的利用细节已经被公开。该漏洞影响 Web 浏览器中运行的 Java SE——基于 Windows、Solaris、Linux 和 Mac OS 平台的 Java SE 7 Update 97，8 Update 73，74，而不是加载和运行可信代码的 Java 部署。

参考链接：<http://www.freebuf.com/news/99973.html>

2. 苹果新品发布会特意提到 iOS 升级

研究人员 Matthew Green 透露，在 iOS 系统中存在一个零日漏洞可以允许攻击者解密截获的 iMessage 信息。Matthew Green 并没有提供具体的漏洞细节，以供苹果公司对其进行修复。该专家补充道：这个安全漏洞对于想要解锁手机的 FBI 可能没有什么帮助。执法者只能使用该漏洞访问使用 iMessage 发送照片和视频的犯罪嫌疑人。苹果表示发布的 iOS 9.3beta 版本将修复这个漏洞。

参考链接：<http://www.freebuf.com/news/99638.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