国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 02 月 15 日-2016 年 02 月 21 日 **2016 年第 8 期**

本周漏洞基本情况

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 298 个，其中高危漏洞 99 个、中危漏洞 186 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 251 个。本周收录的漏洞中，已有 258 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“LEADTOOLS ActiveX control DLL 加载任意代码执行漏洞”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。

成员单位报送漏洞统计

本周，共 5 家成员单位、合作伙伴及个人报送了本周收录的全部 298 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、绿盟科技、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 403 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)	126	126
安天实验室	71	0
绿盟科技	37	0
恒安嘉新	40	0
H3C	4	0

High-Tech Bridge Security Research Lab	5	5
乌云	205	205
漏洞盒子	31	31
CNCERT 安徽分中心	5	5
CNCERT 甘肃分中心	4	4
个人	27	27
报送总计	555	403
录入总计	298（去重）	403

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、Google 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	32	11%
2	Adobe	29	10%
3	Google	21	7%
4	IBM	20	7%
5	Cisco	12	4%
6	Mozilla	11	4%
7	Foxit	10	3%
8	Linux	10	3%
9	Ruby on Rails	9	3%
10	其他	144	48%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 298 个漏洞。其中应用程序漏洞 222 个，操作系统漏洞 37 个，Web 应用漏洞 20 个，网络设备漏洞 18 个，安全产品 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	222

操作系统漏洞	37
Web 应用漏洞	20
网络设备漏洞	18
安全产品漏洞	1

表 3 漏洞按影响类型统计表

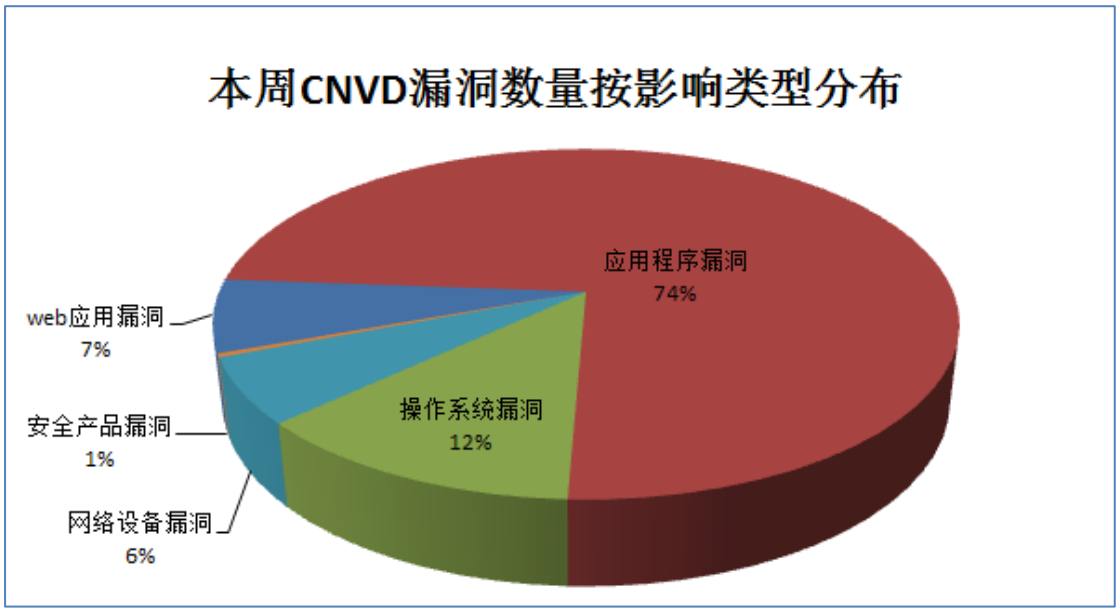

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 20 个电信行业漏洞、14 个移动互联网行业漏洞、5 个工控系统行业漏洞（如下图表所示）。其中，“Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞、Android mediaserver 任意代码执行漏洞、Android 'Qualcomm Performance Module'提权漏洞、Android Qualcomm WiFi Driver 权限提升漏洞、Android Setup Wizard 权限提升漏洞（CNVD-2016-00872、CNVD-2016-00871）、Android 'Debuggerd'权限提升漏洞、Android Mediaserver 权限提升漏洞、Android 内存错误引用漏洞（CNVD-2016-01054）、Android 内存破坏漏洞（CNVD-2016-01097、CNVD-2016-01096、CNVD-2016-01099、CNVD-2016-01098）、Siemens SIMATIC S7-1500 拒绝服务漏洞（CNVD-2016-00931）”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2016-00863	Huawei E5186 4G LTE Router 安全绕过漏洞	中	是
电信	CNVD-2016-00911	KDDI HOME SPOT CUBE devices 存在未明漏洞（CNVD-2016-00911）	中	是
电信	CNVD-2016-00912	KDDI HOME SPOT CUBE devices 存在未明漏洞	中	是

电信	CNVD-2016-00913	KDDI HOME SPOT CUBE devices 跨站请求伪造漏洞	中	是
电信	CNVD-2016-00914	KDDI HOME SPOT CUBE devices CRLF 注入漏洞	中	是
电信	CNVD-2016-00915	KDDI HOME SPOT CUBE devices 开放重定向漏洞	中	是
电信	CNVD-2016-00929	Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞	高	是
电信	CNVD-2016-00992	ISC BIND 9 Supported Preview Edition 拒绝服务漏洞	中	是
电信	CNVD-2016-01056	Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2016-01056）	中	是
电信	CNVD-2016-01062	Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2016-01062）	中	是
电信	CNVD-2016-01064	Cisco Unified Communications Manager SQL 注入漏洞	中	是
电信	CNVD-2016-01069	IBM WebSphere MQ 信息泄露漏洞（CNVD-2016-01069）	低	是
电信	CNVD-2016-01065	Cisco WebEx Meetings Server 存在多个跨站脚本漏洞	中	是
电信	CNVD-2016-01118	IBM WebSphere Portal LDAP 注入漏洞	中	是
电信	CNVD-2016-01117	IBM WebSphere Commerce Enterprise Update Installer 信息泄露漏洞	中	是
电信	CNVD-2016-01124	Cisco Emergency Responder 存在多个跨站脚本漏洞	中	是
电信	CNVD-2016-01125	Cisco Universal Small Cell 设备未授权固件检索漏洞	中	是
电信	CNVD-2016-01126	Cisco IOS 拒绝服务漏洞（CNVD-2016-01126）	中	是
电信	CNVD-2016-01127	Huawei SmartAX MT882 拒绝服务漏洞（CNVD-2016-01127）	中	是
电信	CNVD-2016-01128	Huawei SmartAX MT882 拒绝服务漏洞	中	是
移动互联网	CNVD-2016-00865	Android 安全绕过漏洞	中	是
移动互联网	CNVD-2016-00864	Android mediaserver 任意代码执行漏洞	高	是
移动互联网	CNVD-2016-00870	Android Minikin 库拒绝服务漏洞	低	是
移动互联网	CNVD-2016-00868	Android 'Qualcomm Performance Module' 提权漏洞	高	是
移动互联网	CNVD-2016-00873	Android Qualcomm WiFi Driver 权限提升漏洞	高	是
移动互联网	CNVD-2016-00872	Android Setup Wizard 权限提升漏洞（CNVD-2016-00872）	高	是
移动互联网	CNVD-2016-00871	Android Setup Wizard 权限提升漏洞（CNVD-2016-00871）	高	是

移动互联网	CNVD-2016-00876	Android 'Debuggerd'权限提升漏洞	高	是
移动互联网	CNVD-2016-00875	Android Mediaserver 权限提升漏洞	高	是
移动互联网	CNVD-2016-01054	Android 内存错误引用漏洞（CNVD-2016-01054）	高	是
移动互联网	CNVD-2016-01097	Android 内存破坏漏洞（CNVD-2016-01097）	高	是
移动互联网	CNVD-2016-01096	Android 内存破坏漏洞（CNVD-2016-01096）	高	是
移动互联网	CNVD-2016-01099	Android 内存破坏漏洞（CNVD-2016-01099）	高	是
移动互联网	CNVD-2016-01098	Android 内存破坏漏洞（CNVD-2016-01098）	高	是
工控系统	CNVD-2016-00930	Siemens SIMATIC S7-1500 绕过机制漏洞	低	是
工控系统	CNVD-2016-00931	Siemens SIMATIC S7-1500 拒绝服务漏洞（CNVD-2016-00931）	高	是
工控系统	CNVD-2016-00979	Sauter moduWeb Vision Web 服务器跨站脚本漏洞	中	是
工控系统	CNVD-2016-00978	Sauter moduWeb Vision 安全绕过漏洞	中	是
工控系统	CNVD-2016-00977	Sauter moduWeb Vision 证书不安全存放漏洞	中	是

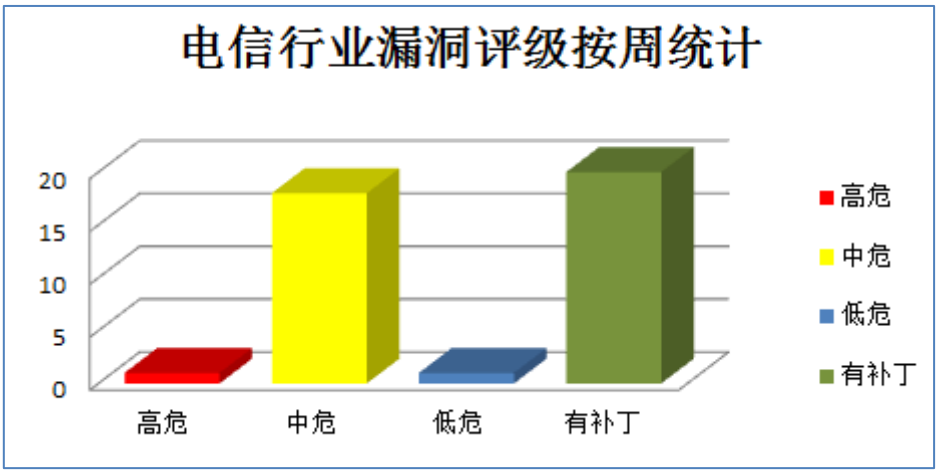

图 1 电信行业漏洞统计

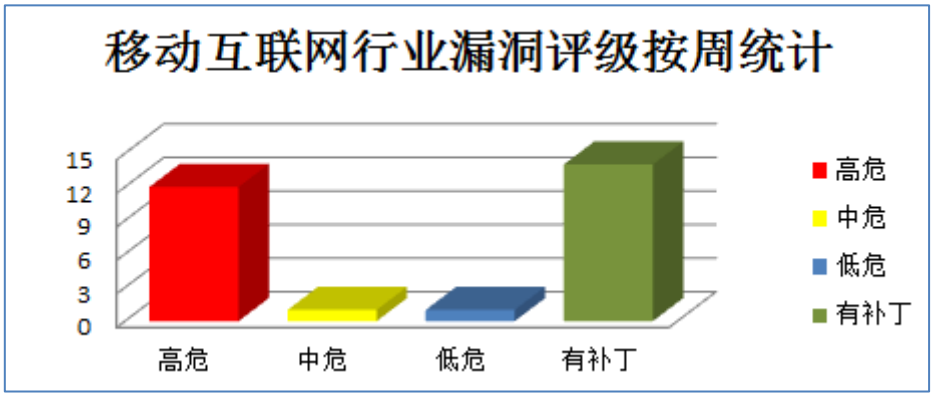

图 2 移动互联网行业漏洞统计

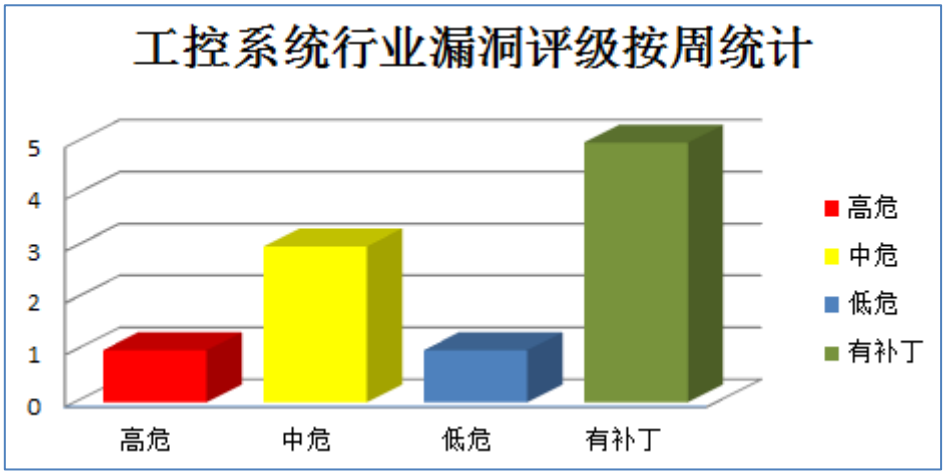

图 3 工控系统行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Cisco 产品安全漏洞

Cisco ASA 是一款自适应安全设备，可提供安全和 VPN 服务的模块化平台，可提供防火墙、IPS、anti-X 和 VPN 服务。Cisco Emergency Responder 实时位置地址跟踪数据库和增强的路由功能可以根据呼叫者的位置，将紧急呼叫直接转移到相应的公共安全应答点（PASP）。Cisco Universal Small Cell Solution 是一个端到端架构，集成了 3G、LTE、电信级 Wi-Fi 及 SON 技术，实现安全有效的异构网络。Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。Cisco Unity Connection（UC）是美国思科（Cisco）公司的一套语音留言平台。该平台可利用语音命令，以“免提”方式拨打电话或者收听留言。Cisco Unified Communications Manager 是美国思科（Cisco）公司的 IP Telephony 解决方案的呼叫处理组件。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、进行跨站攻击、发起拒绝服务攻击或执行等。

CNVD 收录的相关漏洞包括：Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞、Cisco Emergency Responder 存在多个跨站脚本漏洞、Cisco Universal Small Cell 设备未授权固件检索漏洞、Cisco IOS 拒绝服务漏洞（CNVD-2016-01126）、Cisco Unity Connection 跨站脚本漏洞（CNVD-2016-01055）、Cisco Unified Communications Manager SQL 注入漏洞、Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2016-01056、CNVD-2016-01062）。其中，“Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco Unity Connection 跨站脚本漏洞（CNVD-2016-01055）”外，其余漏洞的修补程序。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-2016-00929

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01124

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01125

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01126

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01055

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01064

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01056

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01062

2、 GNU 产品安全漏洞

GNU glibc 是一款按 LGPL 许可协议发布的开源 C 语言编译程序，是 Linux 操作系统中 C 库的实现。本周，上述产品被披露存在缓冲区溢出漏洞。攻击者利用漏洞可通过构建恶意 dns 服务或使用中间人的方法对受害者发起攻击，对 Linux 终端设备构成安全威胁。

CNVD 收录的相关漏洞包括：GNU glibc getaddrinfo()堆栈缓冲区溢出漏洞、GNU glibc 栈缓冲区溢出漏洞。其中，“GNU glibc getaddrinfo()堆栈缓冲区溢出漏洞”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-2016-01100

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00957

3、 Adobe 产品安全漏洞

Adobe Flash Player& Compiler 是美国奥多比（Adobe）公司的一个集成的多媒体播放器，短小精悍，能够在各种浏览器、操作系统和移动设备上使用。本周，上述产品被披露存在拒绝服务漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Adobe Flash Player& Compiler 拒绝服务漏洞（CNVD-2016-01047、CNVD-2016-01044、CNVD-2016-01045、CNVD-2016-01046、CNVD-2016-01049、CNVD-2016-01050、CNVD-2016-01051、CNVD-2016-01048）。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-2016-01047

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01044

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01045

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01046

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01049

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01050

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01051

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01048

4、FFmpeg 产品安全漏洞

FFmpeg 是 FFmpeg 团队的一套可录制、转换以及流化音视频的完整解决方案。本周，上述产品被披露存在拒绝服务漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：FFmpeg 拒绝服务漏洞（CNVD-2016-01129、CNVD-2016-01130、CNVD-2016-01131、CNVD-2016-01132）、FFmpeg 'jpeg2000_decode_tile' 函数拒绝服务漏洞。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-2016-01129

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01130

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01131

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01132

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01000

5、PHP File Manager ‘phpfm.php’身份验证绕过漏洞

PHP File Manager 是一套使用 PHP 脚本管理 Web 站点的应用程序。本周，PHP File Manager 被披露存在身份验证绕过漏洞，攻击者可利用漏洞获取有效的会话，使用受限功能执行 shell 命令。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-2016-00975

更多高危漏洞如表 3 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-2016-00861	WordPress eshop 插件 SQL 注入漏洞	高	用户可联系供应商获得补丁信息：https://wordpress.org/
CNVD-2016-00879	NTP Cronjob Script 本地提权漏洞	高	暂无
CNVD-2016-00885	多款 F5 BIG-IP 产品任意文件上传漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.f5.com/kb/en-us/solutions/public/k/49/sol49580002.html
CNVD-2016-00893	phpMyAdmin 安全绕过漏洞（CNVD-2016-00893）	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.phpmyadmin.net/
CNVD-2016-00900	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2016-00900）	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.mozilla.org/security/announce/2016/mfsa2016-03.html

CNVD-2016-00902	Mozilla Firefox 代码执行漏洞（CNVD-2016-00902）	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.mozilla.org/security/announce/2016/mfsa2016-01.html
CNVD-2016-00903	Mozilla Firefox 代码执行漏洞（CNVD-2016-00903）	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.mozilla.org/security/announce/2016/mfsa2016-01.html
CNVD-2016-00910	Apple OS X AppleGraphicsPowerManagement 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://support.apple.com/HT205731
CNVD-2016-00917	Foxit Reader XFA FormCalc replace 整数溢出远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.foxitsoftware.com/support/security-bulletins.php
CNVD-2016-00918	Foxit PhantomPDF WillClose 内存错误引用远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.foxitsoftware.com/support/security-bulletins.php

表 3 部分高危漏洞列表

小结：本周，Cisco 被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、进行跨站攻击和发起拒绝服务攻击等。另外，GNU、Adobe、FFmpeg 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和发起拒绝服务攻击等。此外，PHP File Manager 被披露存在一个高危漏洞，攻击者可利用漏洞获取有效的会话，使用受限功能执行 shell 命令。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、McAfee 修补 Vulnerability Manager 产品漏洞

McAfee Vulnerability Manager 是美国迈克菲公司的一套安全风险管理解决方案。

本周，McAfee 修补了上述产品存在的跨站请求伪造漏洞，避免攻击者构建恶意 URI，诱使用户解析，可以目标用户上下文执行恶意操作。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/71249

本周要闻速递

1. Adobe Creative Cloud 漏洞导致 Mac 用户数据删除

Adobe 系统已经暂停了对 Creative Cloud 图形服务的某个版本更新。有报道称，有一个 Mac 版本的 Creative Cloud 服务会不经过用户允许，直接越权删除本地的用户数据。据 Backblaze 官方所述，这个自删除漏洞需要 Mac 用户更新该 Adobe 的补丁，然后登录 Adobe 服务才能触发。在登录后，由 Creative Cloud 激活的某个脚本，会删除 Mac 电脑根目录下第一顺位（按字母顺序）的子目录。Backblaze 用户深受该漏洞影响，因为备份服务会将数据存储在根目录的隐藏目录.bzvol。这个隐藏目录按字母排序的话，正好是根目录的第一个目录，因此这批用户遭遇的就不仅是软件包被删除那么简单了。

参考链接：http://www.freebuf.com/news/96332.html

2. 新型 word 文档恶意勒索软件出现，每日可感染达十万台计算机

如果你最近收到一封邮件，而这封邮件里面包含一个微软 word 文档，那么你很有可能已经感染了微软宏病毒。恶意攻击者会开展社会工程学攻击，或通过发送引人注目的垃圾邮件，接下来会诱导受害者访问虚假网站在其系统中安装一款恶意软件“Locky”。如果你发现你的电脑中出现了文件后缀名为.locky 的文件，那么你就感染了该恶意软件，接下来你可以做两件事情，要么按照提示支付赎金，要么重现安装系统。该款恶意软件以 4000 台/小时速度传播，这意味着每天会出现 100000 台新感染的计算机。

参考链接：http://www.freebuf.com/news/96570.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