国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 02 月 20 日-2017 年 02 月 26 日 **2017 年第 9 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**高**。

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 340 个，其中高危漏洞 149 个、中危漏洞 179 个、低危漏洞 12 个。漏洞平均分值为 6.41。本周收录的漏洞中，涉及 0day 漏洞 125 个（占 37%）。其中互联网上出现“Microsoft Edge 内存破坏漏洞（CNVD-2017-01981）、EMC Documentum D2 远程代码执行漏洞”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。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 504 个，与上周（761 个）环比下降 34%。

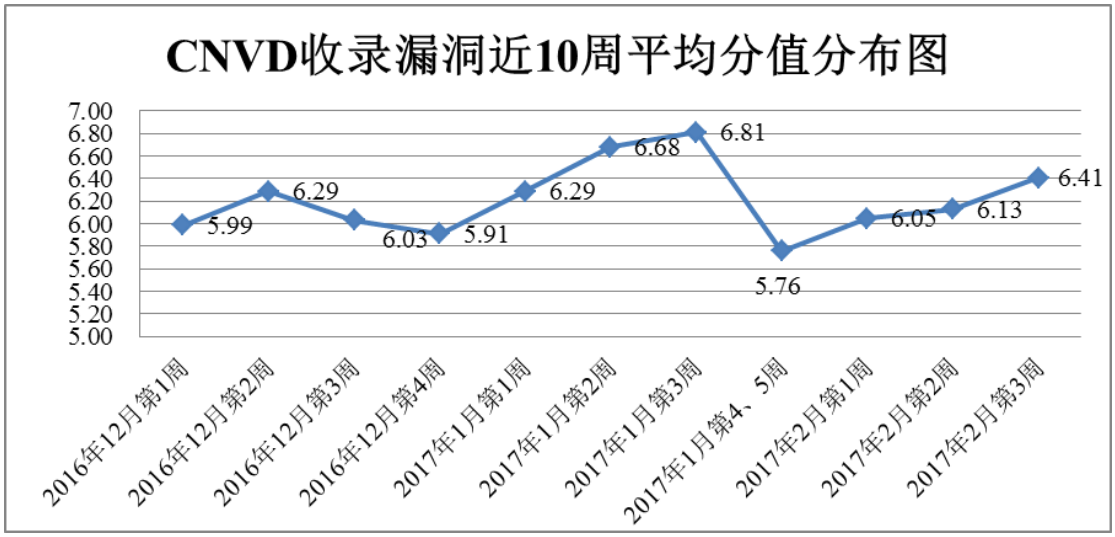

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 340 个漏洞。报送情况如表 1 所示。其中，安天实验室、蓝盾信息安全技术有限公司、启明星辰、天融信等单位报送数量较多。360 网神、漏洞盒子、工业和信息化部电子第五研究所信息安全研究中心、江苏省信息安全测评中心及其他个人白帽子向 CNVD 提交了 50

4 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
安天实验室	161	0
蓝盾信息安全技术有限公司	116	9
启明星辰	114	4
天融信	107	0
H3C	95	0
华为技术有限公司	90	0
360 网神	56	56
绿盟科技	41	0
杭州安恒信息技术有限公司	38	15
中国电信集团系统集成有限责任公司	32	0
安全狗	27	0
恒安嘉新	21	0
北京数字观星科技有限公司	5	0
深圳市腾讯计算机系统有限公司（玄武实验室）	3	3
西安四叶草信息技术有限公司	1	1
漏洞盒子	287	287
工业和信息化部电子第五研究所信息安全研究中心	6	6
江苏省信息安全测评中心	1	1
CNCERT 江西分中心	26	26
CNCERT 山西分中心	24	24

CNCERT 宁夏分中心	11	11
CNCERT 重庆分中心	10	10
CNCERT 陕西分中心	6	6
CNCERT 四川分中心	5	5
CNCERT 吉林分中心	4	4
CNCERT 甘肃分中心	2	2
CNCERT 福建分中心	2	2
CNCERT 广东分中心	1	1
CNCERT 新疆分中心	1	1
CNCERT 湖南分中心	1	1
CNCERT 海南分中心	1	1
个人	28	28
报送总计	1323	504
录入总计	340（去重）	504

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 340 个漏洞。其中应用程序漏洞 196 个，web 应用漏洞 85 个，操作系统漏洞 26 个，网络设备漏洞 25 个，安全产品漏洞 7 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	196
web 应用漏洞	85
操作系统漏洞	26
网络设备漏洞	25
安全产品漏洞	7
数据库漏洞	1

表 2 漏洞按影响类型统计表

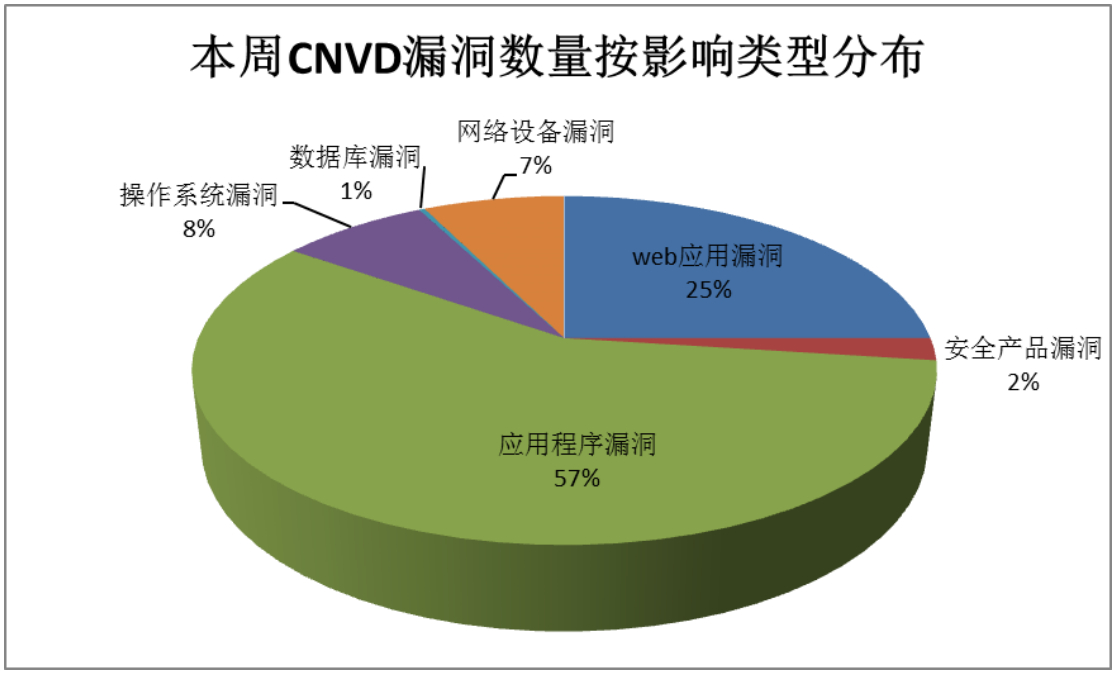

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Joomla、Cisco 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	24	7%
2	Joomla	24	7%
3	Cisco	21	6%
4	Google	16	5%
5	Apple	17	5%
6	Qemu	14	4%
7	NVIDIA	11	3%
8	Linux	10	3%
9	ZZIPlib	8	2%
10	其他	195	58%

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 18 个电信行业漏洞，23 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“多款 TP-Link 路由器存在多个漏洞、D-Link DGS-1510 Switches 存在认证绕过漏洞、BINOM3 Electric Power Quality Meter 信息泄露漏

洞、BINOM3 Electric Power Quality Meter 硬编码漏洞、Google Android AOSP Messaging 信息泄露漏洞（CNVD-2017-01773）、TYPO3 任意代码执行漏洞（CNVD-2017-01648）、Google Android Mediaserver 特权提升漏洞”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/

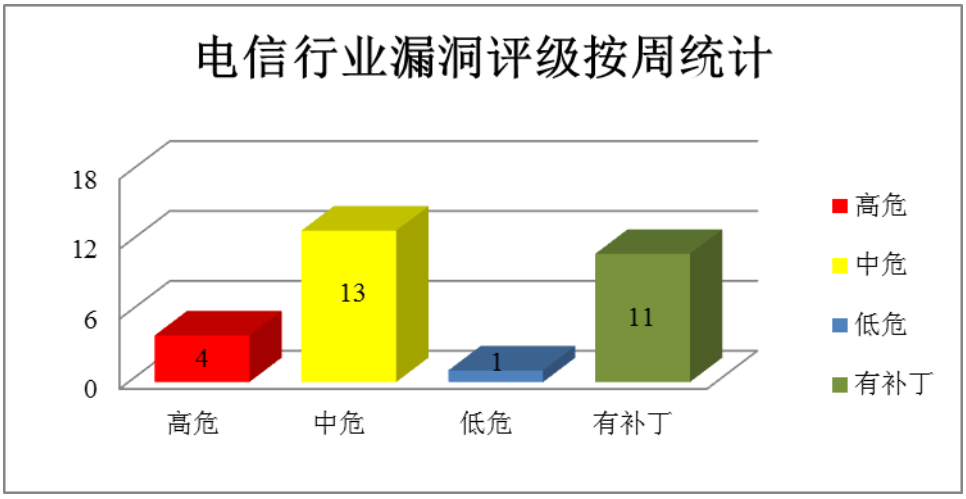

图 3 电信行业漏洞统计

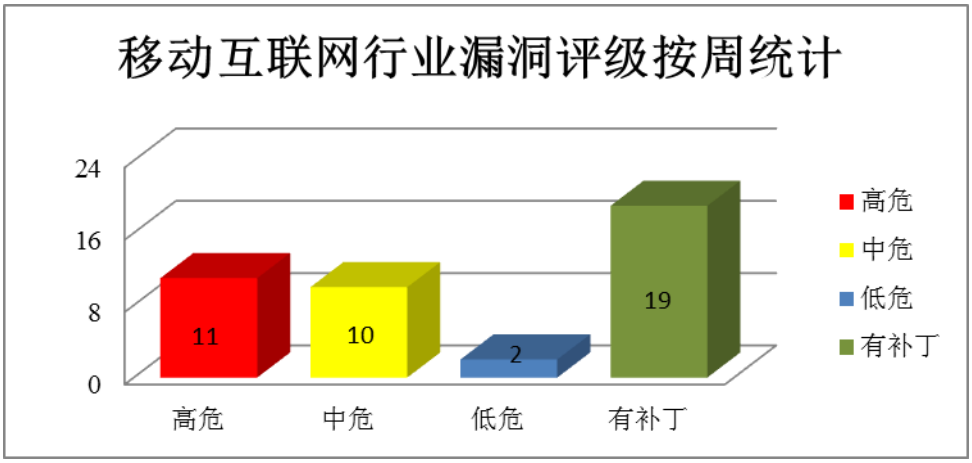

图 4 移动互联网行业漏洞统计

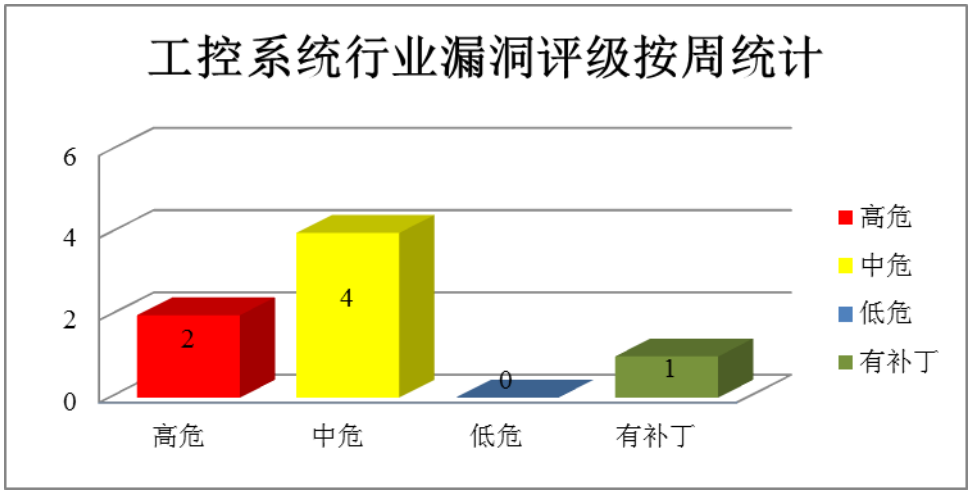

图 5 工控系统行业漏洞统计

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、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，该产品被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击或获取权限执行任意代码。

CNVD 收录的相关漏洞包括：Linux kernel 特权提升漏洞、Linux Kernel 不完全修复本地权限提升漏洞、Linux Kernel 'net/sctp/socket.c'本地拒绝服务漏洞、Linux Kernel 'drivers/infiniband/sw/rxe/rxe_mr.c'本地整数溢出漏洞、Linux kernel 'include/linux/init_task.h'拒绝服务漏洞、Linux kernel 拒绝服务漏洞（CNVD-2017-01859、CNVD-2017-01852）、Linux kernel 'ip6_gre.c'拒绝服务漏洞。其中，“Linux kernel 特权提升漏洞、Linux Kernel 不完全修复本地权限提升漏洞、Linux Kernel 'net/sctp/socket.c'本地拒绝服务漏洞、Linux Kernel 'drivers/infiniband/sw/rxe/rxe_mr.c'本地整数溢出漏洞”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-2017-01870

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01986

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01989

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01990

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01991

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01859

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01852

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01603

2、Adobe 存在产品安全漏洞

Adobe Flash Player 是美国 Adobe 公司开发的一款广泛使用的、专有的多媒体程序播放器。本周，该产品被披露存在缓冲区溢出和内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存破坏漏洞（CNVD-2017-01781、CNVD-2017-01782、CNVD-2017-01783、CNVD-2017-01784）、Adobe Flash Player 堆缓冲区溢出漏洞（CNVD-2017-01785、CNVD-2017-01786、CNVD-2017-01787）、Adobe Flash Player 整数溢出漏洞（CNVD-2017-01780）。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-2017-01781
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01782
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01783
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01784
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01785
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01786
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01787
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01780

3、Google 产品安全漏洞

Google Nexus/Pixel 都是美国谷歌（Google）公司的智能手机。Google Nexus 9 是美国谷歌（Google）公司的一款平板电脑。NVIDIA GPU Drivers 是一个图形处理器驱动。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞以提升的内核权限执行任意代码。

CNVD 收录的相关漏洞包括：Google Nexus/Pixel 产品 Qualcomm Wi-Fi Driver 权限提升漏洞、Google Nexus/Pixel 产品 Qualcomm Wi-Fi Driver 权限提升漏洞（CNVD-2017-01580、CNVD-2017-01581、CNVD-2017-01582、CNVD-2017-01583、CNVD-2017-01584）、Google Nexus NVIDIA GPU Driver 权限提升漏洞（CNVD-2017-01588、CNVD-2017-01589）。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-2017-01585
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01580
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01581
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01582
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01583
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01584

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01588

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01589

4、Apple 产品安全漏洞

Apple macOS Sierra 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统。Help Viewer 是其中的一个基于 WebKit 的 HTML 查看器。Bluetooth 是一个蓝牙组件。Graphics Driver 是一个图形驱动器组件。Apple Safari 是美国苹果公司的一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发起跨站脚本攻击或执行任意代码等。

CNVD 收录的相关漏洞包括：Apple macOS Sierra Help Viewer 跨站脚本漏洞、Apple macOS Sierra Bluetooth 内存错误引用漏洞、Apple macOS Sierra Graphics Driver 内存破坏漏洞、Apple Safari WebKit 内存破坏漏洞（CNVD-2017-01634、CNVD-2017-01635、CNVD-2017-01636、CNVD-2017-01685）、Apple Safari WebKit 内存初始化漏洞。除“Apple macOS Sierra Help Viewer 跨站脚本漏洞”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-2017-01572

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01573

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01450

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01451

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01487

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01488

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01485

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01486

5、TP-Link C2 和 C20i 默认凭证设计漏洞

TP-Link 是一家中国网络设备制造商，如路由器、IOT 设备等。本周，TP-Link 被披露存在默认凭证设计漏洞。攻击者可利用漏洞执行多次 system()命令，并以 root 权限运行。目前，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-2017-01722

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-2017-01602	GNU Bash 存在多个任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			http://seclists.org/oss-sec/2017/q1/334
CNVD-2017-01640	ChatSecure 和 Zom 用户模拟漏洞	高	用户可联系供应商获得补丁信息： https://zom.im/ https://chatsecure.org/
CNVD-2017-01641	Yaxim 和 Bruno 用户模拟漏洞	高	用户可联系供应商获得补丁信息： https://yaxim.org/ https://yaxim.org/bruno/
CNVD-2017-01648	TYPO3 任意代码执行漏洞（CNVD-2017-01648）	高	用户可联系供应商获得补丁信息： https://forge.typo3.org/issues/79326
CNVD-2017-01649	Firejail Incomplete Fix 本地权限提升漏洞	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： https://firejail.wordpress.com/
CNVD-2017-01760	OIC Exponent CMS 远程代码执行漏洞（CNVD-2017-01760）	高	厂商已发布漏洞修复程序，请及时关注更新： http://www.openwall.com/lists/oss-security/2016/09/29/11
CNVD-2017-01872	OpenStack Nova-LXD 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://seclists.org/oss-sec/2017/q1/347
CNVD-2017-01886	多款 SAP 产品内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://service.sap.com/sap/support/notes/2391018
CNVD-2017-01933	DotCMS SQL 注入漏洞（CNVD-2017-01933）	高	厂商已发布了漏洞修复程序，请及时关注更新： http://dotcms.com/security/SI-39
CNVD-2017-02022	SAP HANA 存在多个漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://service.sap.com/sap/support/notes/2407694

表 4 部分重要高危漏洞列表

小结：本周，Linux 被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击或获取权限执行任意代码。此外，Adobe、Google、Apple 等多款产品被披露存在多个漏洞，攻击者利用漏洞可提升权限、发起跨站脚本攻击或执行任意代码等。另外，TP-Link 被披露存在默认凭证设计漏洞。攻击者可利用漏洞执行多次 system()命令，并以 root 权限运行。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. 访问一个网站就能让 ASLR 保护失效，百万设备陷入危机

安全研究员发现一个芯片漏洞，此漏洞影响到数以百万计的设备，不管设备上安装

的是什么操作系统或是应用程序，这个漏洞都能让设备的防黑保护无效化。该漏洞存在于内存管理单元（MMU）（许多 CPU 的组件）的工作方式中，利用此漏洞就能绕过地址空间布局随机化（ASLR）保护。更糟糕的是，这个漏洞不会因为任何的软件升级而被彻底修复。

参考链接：http://www.freebuf.com/vuls/127229.html

2. Python 与 Java 曝漏洞，黑客利用 FTP 注入攻击可绕过防火墙

上周六，安全研究员 Alexander Klink 公布了一种很有趣的攻击方式，他利用 Java 应用中的 XXE(XML External Entity)漏洞发送邮件。看到 Klink 的攻击后，来自 Blindspot Security 的研究员 Timothy Morgan 又公开了一种类似的攻击方式，这种攻击方式能够针对 Java 和 Python 的 FTP——由于该攻击可被用来绕过防火墙，因此更为严重。这种攻击和利用了缺少 CRLF 过滤特性注入恶意 FTP 命令的方法是类似的。用户应该禁用浏览器的 Java 插件并且取消.jnlp 文件与 Java Web Start 的关联。

参考链接：http://www.freebuf.com/vuls/127595.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