

信息安全漏洞周报

2017 年 06 月 19 日-2017 年 06 月 25 日

2017 年第 26 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 326 个，其中高危漏洞 128 个、中危漏洞 172 个、低危漏洞 26 个。漏洞平均分为 6.17。本周收录的漏洞中，涉及 0day 漏洞 60 个（占 18%），其中互联网上出现“IPFire 远程执行代码漏洞、CMS Made Simple 远程代码执行漏洞”等零日代码攻击漏洞。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 1336 个，与上周（1342 个）基本持平。

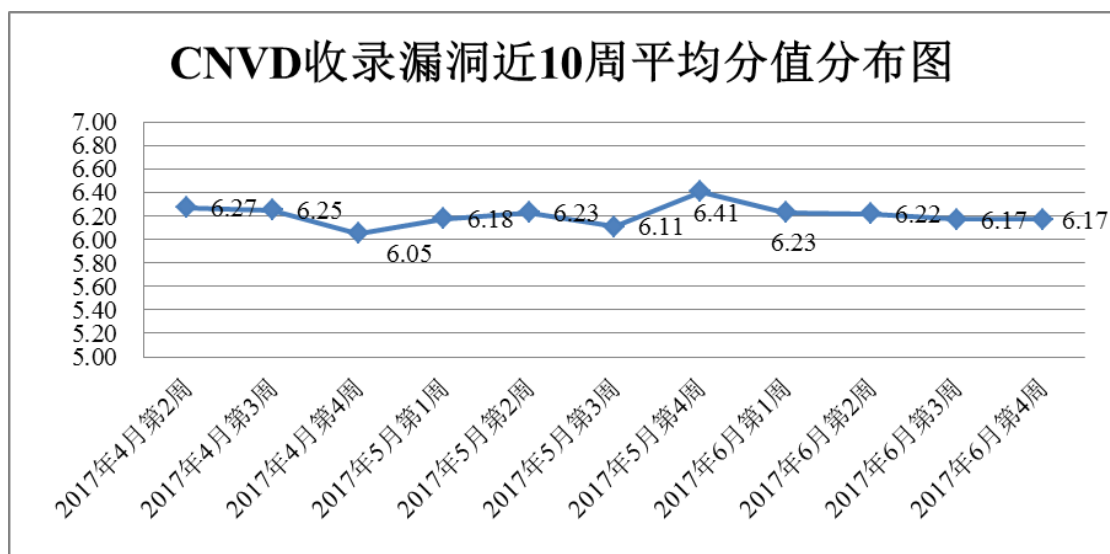


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 19 家成员单位、企业用户及个人用户报送了本周收录的全部 326 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、天融信、华为技术有限公司、绿盟科技等单位报送数量较多。360 网神、漏洞盒子、南京联成科技发展有限公司、

广州神月信息技术有限公司、中新网络信息安全股份有限公司、江苏君立华域信息安全技术有限公司、福建六壬网安股份有限公司、北京山石网科信息技术有限公司、清远职业技术学院、江苏同袍信息科技有限公司、广州软云计算机科技有限公司、河北网信智安信息技术有限公司、长沙天融信网络安全技术有限公司、安徽新华博信息技术股份有限公司、北京奇虎测腾科技有限公司及其他个人白帽子向 CNVD 提交了 1336 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
360 网神	289	289
安天实验室	147	0
恒安嘉新	120	0
天融信	113	0
华为技术有限公司	107	1
绿盟科技	101	0
中国电信集团系统集成有限责任公司	75	0
漏洞盒子	68	68
阿里云计算有限公司	49	49
杭州安恒信息技术有限公司	36	0
H3C	27	0
厦门服云信息科技有限公司	21	0
启明星辰	8	8
北京无声信息技术有限公司	7	0
北京数字观星科技有限公司	5	0
广西鑫瀚科技有限公司	4	4
知道创宇	3	3
南京铤迅信息技术股份有限公司	1	1

西安四叶草信息技术有限公司	1	1
南京联成科技发展股份有限公司	79	79
广州神月信息安全技术有限公司	56	56
中新网络信息安全股份有限公司	33	33
江苏君立华域信息安全技术有限公司	26	26
福建六壬网安股份有限公司	25	25
北京山石网科信息技术有限公司	19	19
清远职业技术学院	16	16
江苏同袍信息科技有限公司	13	13
广州软云计算科技有限公司	9	9
河北网信智安信息技术有限公司	6	6
长沙天融信网络安全技术有限公司	4	4
安徽新华博信息技术股份有限公司	1	1
北京奇虎测腾科技有限公司	1	1
吉林分中心	4	4
北京分中心	3	3
新疆分中心	2	2
广东分中心	1	1
陕西分中心	1	1
浙江分中心	1	1
个人	612	612
报送总计	2094	1336

录入总计	326（去重）	1336
------	---------	------

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 326 个漏洞。其中应用程序漏洞 217 个，web 应用漏洞 45 个，操作系统漏洞 38 个，网络设备漏洞 20 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	217
web 应用漏洞	45
操作系统漏洞	38
网络设备漏洞	20
安全产品漏洞	6

表 2 漏洞按影响类型统计表

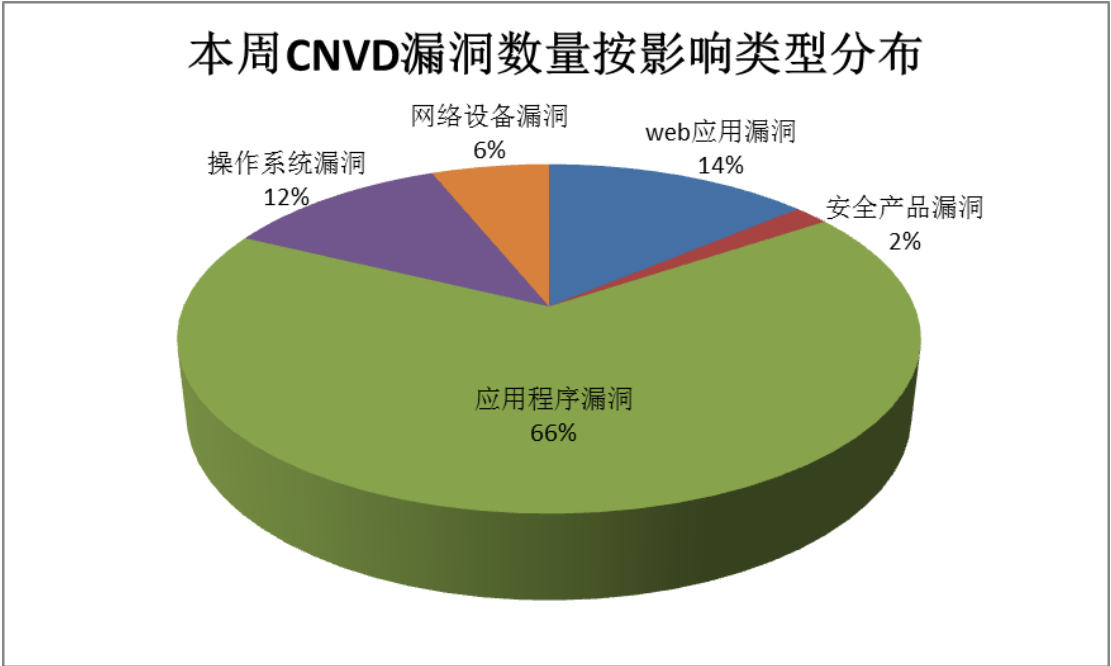


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、Wireshark 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	Google	34	10%
2	Adobe	19	6%
3	Wireshark	13	4%
4	Apple	12	4%

5	SAP	9	3%
6	WordPress	8	2%
7	Fortinet	7	2%
8	IBM	6	2%
9	GNU	6	2%
10	其他	212	65%

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 11 个电信行业漏洞，46 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，“多款 Zyxel 产品远程拒绝服务漏洞、Sierra Wireless GX440 命令注入漏洞、Sierra Wireless GX440 权限提升漏洞、MiniUPnP MiniUPnPc 拒绝服务漏洞、Apple WebKit 远程代码执行漏洞、Google Android Bluetooth 提权漏洞、Trihedral VTScada 跨站脚本漏洞、Trihedral VTScada 拒绝服务漏洞”等的综合评级为“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/>

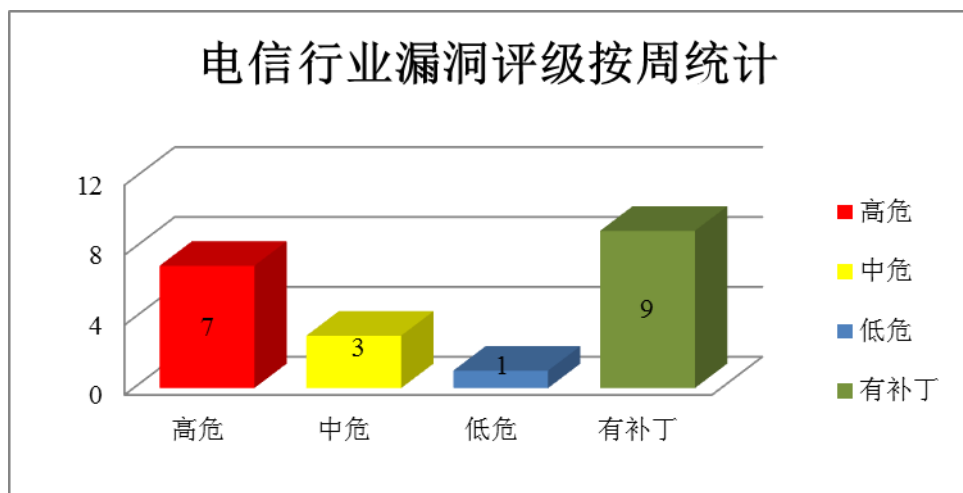


图 3 电信行业漏洞统计

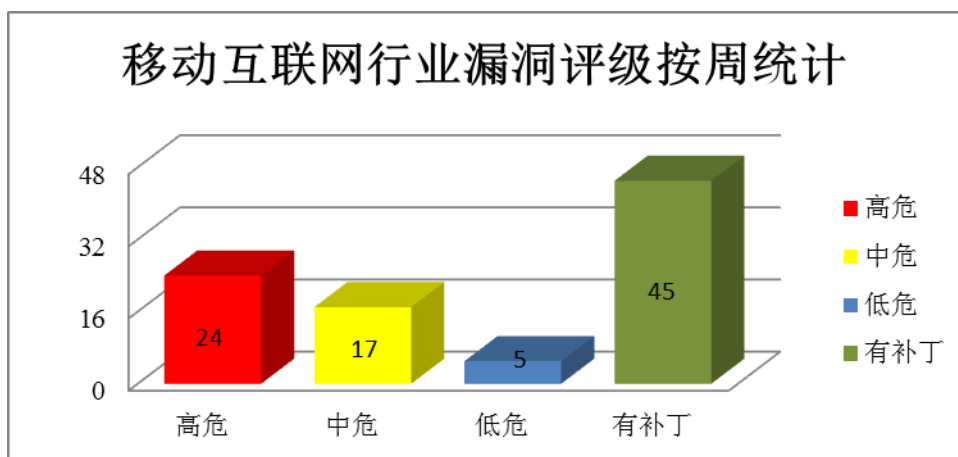


图 4 移动互联网行业漏洞统计

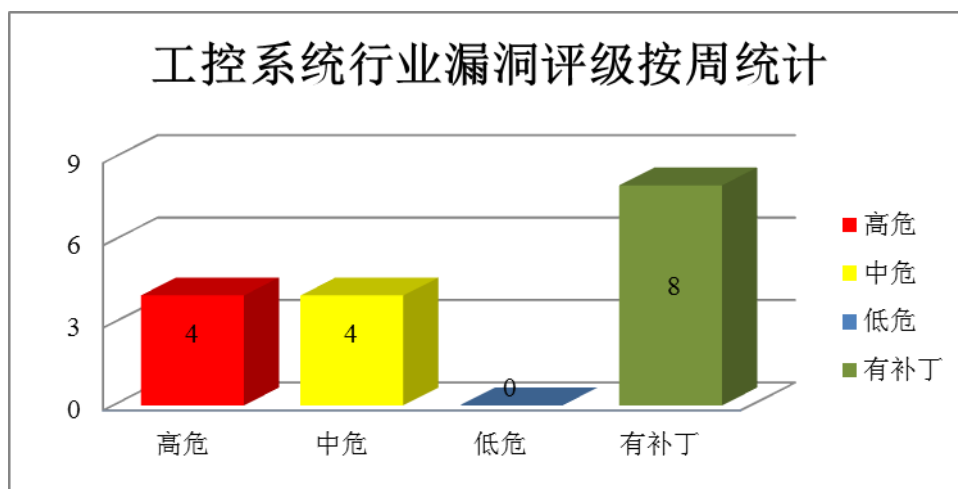


图 5 工控系统行业漏洞统计

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 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。Adobe Digital Editions（DE）是一套电子书阅读管理软件。本周，上述产品被披露存在内存破坏漏洞，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 Digital Editions 内存破坏漏洞、Adobe Digital Editions 内存破坏漏洞（CNVD-2017-10147、CNVD-2017-10148）、Adobe Flash Player 内存破坏漏洞（CNVD-2017-10259、CNVD-2017-10260、CNVD-2017-10261、CNVD-2017-10262、CNVD-2017-10263）。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-2017-10149>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10147>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10148>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10259>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10260>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10261>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10262>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10263>

2、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共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm 是使用在其中的一个设备专用的高通组件。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 权限提升漏洞（CNVD-2017-10801、CNVD-2017-10802、CNVD-2017-10805、CNVD-2017-10806、CNVD-2017-10808）、Google Android Qualcomm 组件存在未明漏洞（CNVD-2017-11062、CNVD-2017-11063、CNVD-2017-11064）。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-2017-10801>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10802>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10805>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10806>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10808>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11062>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11063>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11064>

3、Apple 产品安全漏洞

Apple Safari 是美国苹果（Apple）公司的一款 Web 浏览器。WebKit 是一套开源 Web 浏览器引擎；Apple iOS 是一套为移动设备所开发的操作系统；macOS Sierra 是一套为 Mac 计算机所开发的专用操作系统。Apple Mac OS X 是为 Mac 计算机所开发的一套专用操作系统。macOS 是一套运行于苹果 Macintosh 系列电脑上的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apple iOS 和 macOS Sierra SQLite 内存破坏漏洞、Apple iOS 和 macOS Sierra SQLite 内存破坏漏洞（CNVD-2017-11050）、Apple macOS Server 用户枚举漏洞、Apple macOS Sierra iBooks 权限提升漏洞（CNVD-2017-10184）、

Apple macOS Sierra Intel 图像驱动权限提升漏洞、Apple macOS Sierra IOGraphics 内存破坏漏洞、Apple Safari 远程拒绝服务漏洞、Apple WebKit 远程代码执行漏洞。除“Apple macOS Server 用户枚举漏洞、Apple macOS Sierra iBooks 权限提升漏洞（CNVD-2017-10184）、Apple Safari 远程拒绝服务漏洞”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-2017-11049>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11050>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10995>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10184>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10183>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10358>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10391>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10709>

4、FortiPortal 产品安全漏洞

FortiPortal 是美国飞塔（Fortinet）公司的高级功能丰富的托管安全分析和安全管理支持器。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞在受影响网站上下文中执行任意脚本代码，窃取基于 cookie 的身份验证，绕过安全限制并执行未授权的操作，将用户重定向到受攻击者控制的网站或者获取敏感信息。

CNVD 收录的相关漏洞包括：FortiPortal 存在多个漏洞（CNVD-2017-10722、CNVD-2017-10723、CNVD-2017-10724、CNVD-2017-10725、CNVD-2017-10726、CNVD-2017-10727）、FortiPortal 存在多个漏洞。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-2017-10722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10723>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10724>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10725>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10726>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10727>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-10728>

5、Microsoft Windows 任意代码执行漏洞（CNVD-2017-10350）

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。本周，Microsoft 被披露存在任意代码执行漏洞，攻击者可利用漏洞在目标计算机上执行任意代码。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-2017-10350>

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-2017-10178	Sierra Wireless GX440 权限提升漏洞	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.sierrawireless.com/
CNVD-2017-10179	Sierra Wireless GX440 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: https://www.sierrawireless.com/
CNVD-2017-10268	KBVault MySQL 任意文件上传漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接: http://kbvaultmysql.codeplex.com/
CNVD-2017-10349	Sophos Cyberoam UTM CR25iNG 安全绕过漏洞	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.sophos.com/
CNVD-2017-10383	PlaySms 远程代码执行漏洞 (CNVD-2017-10383)	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://playsms.org/download/
CNVD-2017-10545	GNU C Library 远程拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页: https://www.gnu.org/
CNVD-2017-10696	Citrix NetScaler Gateway 堆缓冲区溢出漏洞	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.citrix.com/article/CTX222657
CNVD-2017-10708	Trihedral VTScada 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页: https://www.trihedral.com/
CNVD-2017-10711	Pivotal Spring Security Deserialization 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接: https://pivotal.io/security/cve-2017-4995
CNVD-2017-10821	Siemens XHQ 权限提升漏洞	高	用户可联系供应商获得补丁信息: https://www.siemens.com/cert/advisories/

表 4 部分重要高危漏洞列表

小结：本周，Adobe 被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Apple、FortiPortal 等多款产品被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制、提升权限、执行任意命令或发起拒绝服务攻击等。另外，Microsoft 被披

露存在任意代码执行漏洞，攻击者可利用漏洞在目标计算机上执行任意代码。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。



本周漏洞要闻速递

1. Linux 中的 Stack Clash 漏洞，可被黑客利用获取本地 root 权限

上个月，Qualys 的安全研究人员在多种基于 Unix 的系统上发现名为“Stack Clash”的漏洞，该漏洞能让攻击者在 UNIX 系统上获得 root 权限，并接管这台受到攻击的计算机。目前安全研究人员发现了这个缺陷，正与各种供应商合作，尽早发布修复程序。。

参考链接：<http://www.freebuf.com/news/137824.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