国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 01 月 16 日-2017 年 01 月 22 日 **2017 年第 4 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 167 个，其中高危漏洞 82 个、中危漏洞 78 个、低危漏洞 7 个。漏洞平均分值为 6.81。本周收录的漏洞中，涉及 0day 漏洞 11 个（占 7%）。其中互联网上出现“Samsung Smart cam 远程命令执行漏洞”零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 574 个，与上周（549 个）环比增长 5%。

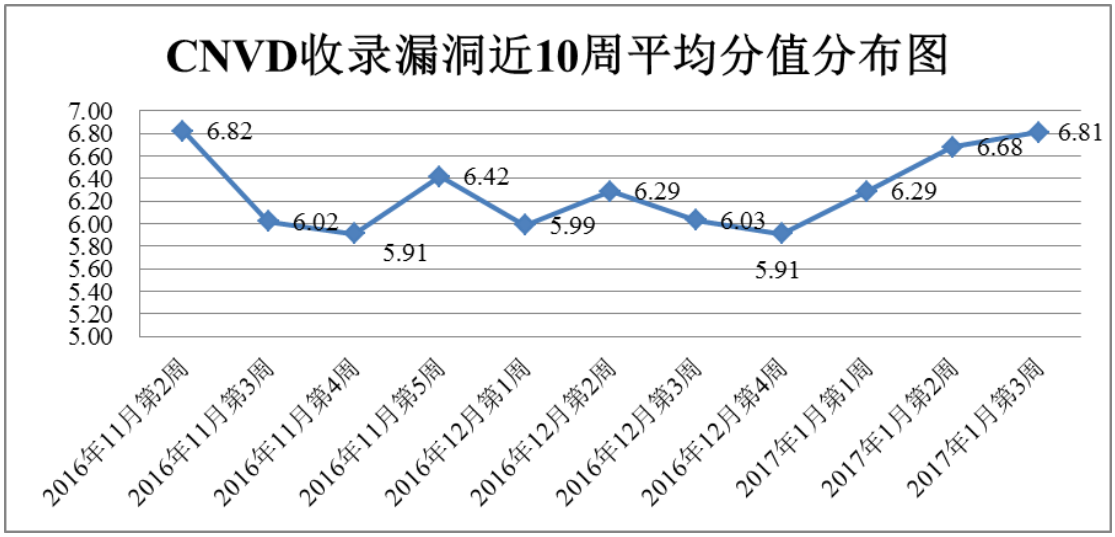

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 12 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 167 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、天融信、华为技术有限公司、启明星辰等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、上海零盾网络科技有限公司、军工保密资格审查认证中心及其他个人白帽子向 CNVD

提交了 574 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	378	378
蓝盾信息安全技术有限公司	220	0
天融信	156	0
华为技术有限公司	111	0
启明星辰	109	1
安天实验室	94	0
H3C	82	0
绿盟科技	45	0
恒安嘉新	27	3
数字观星	6	0
西安四叶草信息技术有限公司	4	4
南京铱迅信息技术股份有限公司	2	2
漏洞盒子	98	98
广西鑫瀚科技有限公司	15	15
军工保密资格审查认证中心	1	1
上海零盾网络科技有限公司	1	1
山西分中心	15	15
上海分中心	14	14
湖南分中心	12	12
江西分中心	7	7
新疆分中心	6	6

福建分中心	1	1
广东分中心	1	1
个人	15	15
报送总计	1420	574
录入总计	167（去重）	574

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 167 个漏洞。其中应用程序漏洞 75 个，操作系统漏洞 50 个，web 应用漏洞 22 个，网络设备漏洞 17 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	75
操作系统漏洞	50
web 应用漏洞	22
网络设备漏洞	17
数据库漏洞	3

表 2 漏洞按影响类型统计表

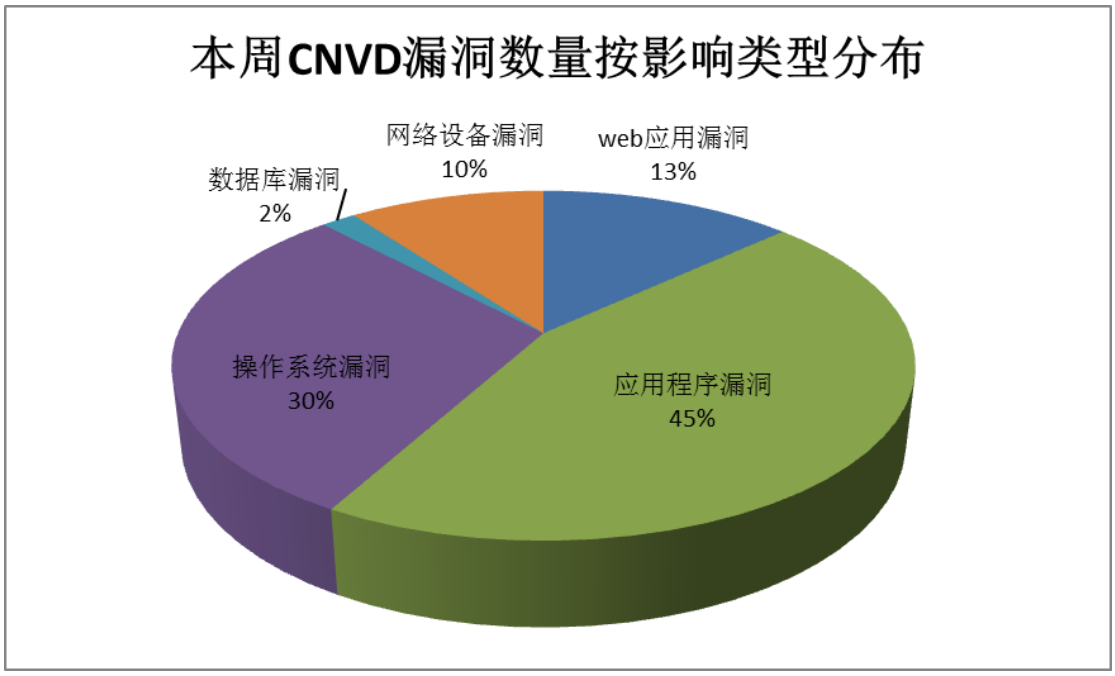

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Oracle、IBM 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	41	25%
2	Oracle	18	11%
3	IBM	13	8%
4	Juniper Networks, Inc.	11	7%
5	Huawei	8	5%
6	WordPress	7	4%
7	libgit2	5	3%
8	Gnu	4	2%
9	Samsung	4	2%
10	其他	56	33%

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 个电信行业漏洞，47 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“IBM WebSphere MQ 远程代码执行漏洞、Advantech WebAccess 'updateTemplate.aspx' SQL 注入漏洞 Google Nexus Broadcom Wi-Fi Driver 权限提升漏洞（CNVD-2017-00571、CNVD-2017-00572、CNVD-2017-00573、CNVD-2017-00574）、Google Android Mediaserver 组件拒绝服务漏洞（CNVD-2017-00532、CNVD-2017-00531）、Google Nexus Broadcom Wi-Fi 驱动权限提升漏洞（CNVD-2017-00578、CNVD-2017-00579）”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/

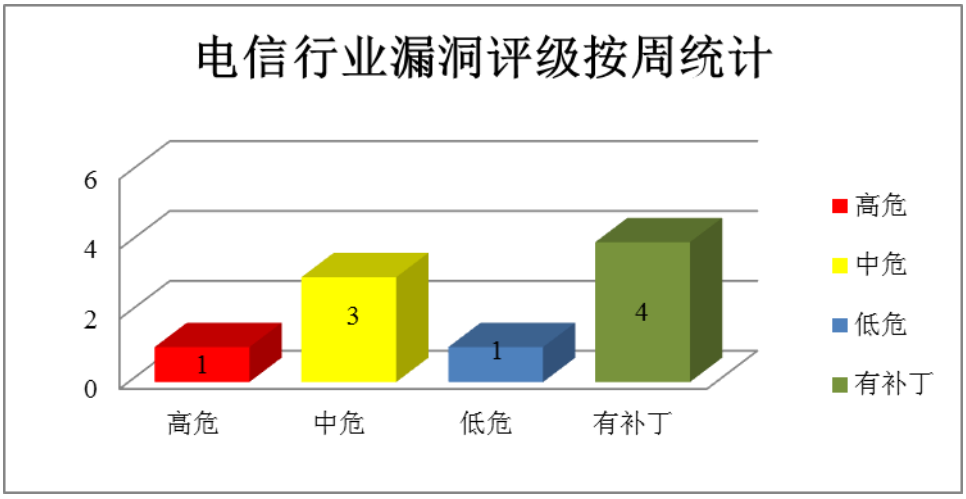

图 3 电信行业漏洞统计

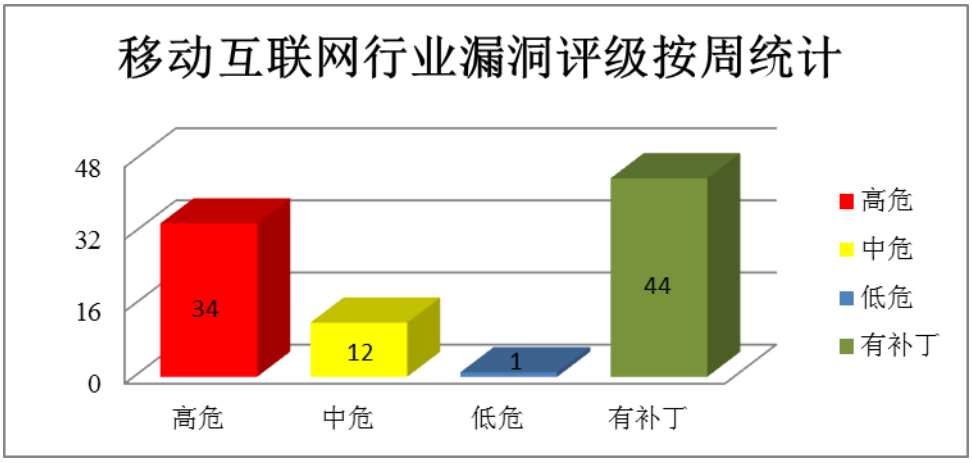

图 4 移动互联网行业漏洞统计

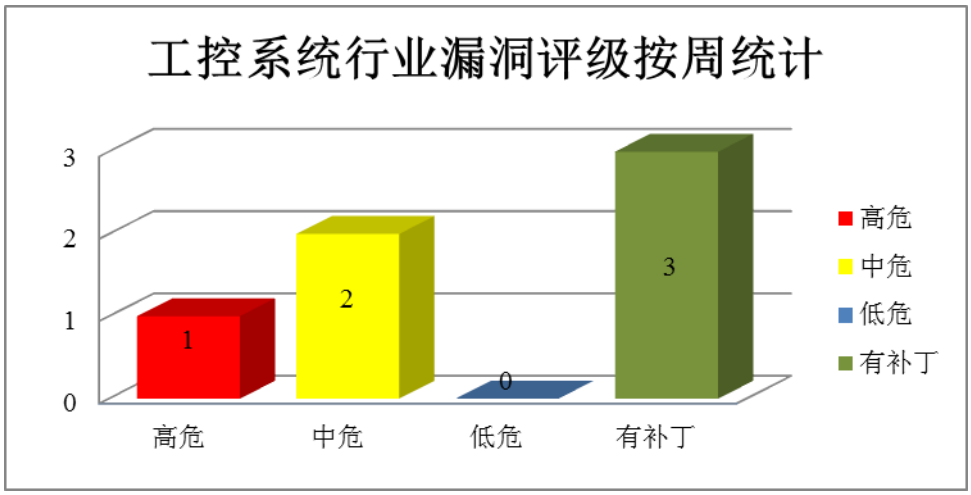

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

1 月 18 日，Oracle 发布了 2017 年 1 月份的安全更新，修复了其多款产品存在的 270 个安全漏洞。受影响的产品包括 Oracle 数据库（2 个）、Oracle Secure Backup（2 个）、Oracle Big Data（1 个）；中间件产品 Fusion Middleware（18 个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（8 个）、电子商务套装软件 OracleE-Business Suite（121 个）、供应链套装软件 Oracle Supply Chain Products Suite（1 个）；PeopleSoft 产品（7 个）、JDEdwards 产品（1 个）、Oracle Siebel 托管型 CRM 软件（3 个）、Oracle Commerce（1 个）、Communications Applications（4 个）、金融服务分析应用软件 Oracle Financial Services Applications（37）、RetailApplications（8 个）、Primavera 产品（4 个）、Java SE（17 个）、Oracle Sun 系统产品（4 个）、Virtualization（4 个）和 MySQL 数据库（27 个）。本次安全更新提供了有 252 个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle E-Business Suite 远程安全漏洞（CNVD-2017-00639、CNVD-2017-00640、CNVD-2017-00641、CNVD-2017-00642、CNVD-2017-00643、CNVD-2017-00644、CNVD-2017-00645、CNVD-2017-00646）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/webinfo/show/4037

2、Google 产品安全漏洞

Android on Nexus 9 是美国谷歌（Google）公司和开放手持设备联盟共同开发的一套运行于 Nexus 9 中并以 Linux 为基础的开源操作系统。NVIDIA camera driver 是使用在其中的一个摄像头驱动程序。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Nexus NVIDIA GPU 驱动权限提升漏洞、Google Nexus NVIDIA GPU 驱动权限提升漏洞（CNVD-2017-00469、CNVD-2017-00470、CNVD-2017-00471、CNVD-2017-00472、CNVD-2017-00473、CNVD-2017-00474、CNVD-2017-00475）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-2017-00468
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00469
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00470
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00471
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00472
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00473
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00474
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00475

3、IBM 产品安全漏洞

IBM Kenexa LMS on Cloud 是美国 IBM 公司的一套可配置的集成了社交网络、协作和知识分享功能的企业级社交学习管理系统 (LMS)。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞更改数据库信息、进行跨站脚本攻击或执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Kenexa LMS on Cloud SQL 注入漏洞（CNVD-2017-00563、CNVD-2017-00564、CNVD-2017-00565）、IBM Kenexa LMS on Cloud 跨站脚本漏洞（CNVD-2017-00561、CNVD-2017-00562）、IBM Kenexa LMS on Cloud 目录遍历漏洞（CNVD-2017-00566、CNVD-2017-00567）、IBM Kenexa LMS on Cloud 任意代码执行漏洞等。除“IBM Kenexa LMS on Cloud 跨站脚本漏洞（CNVD-2017-00561）、IBM Kenexa LMS on Cloud 目录遍历漏洞（CNVD-2017-00566）”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-2017-00563
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00564
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00565
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00561
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00562
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00566
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00567
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00568

4、Juniper Networks 产品安全漏洞

Juniper Junos 是一套专用于该公司的硬件系统的网络操作系统。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、泄露敏感信息或执行任意代码等。

CNVD 收录的相关漏洞包括：Juniper Junos 拒绝服务漏洞（CNVD-2017-00602、CNVD-2017-00603、CNVD-2017-00604、CNVD-2017-00605）、Juniper Junos 权限提升漏洞（CNVD-2017-00606）、Juniper Junos 代码执行漏洞、Juniper Junos 跨站脚本漏洞（CNVD-2017-00608）、Juniper Junos XML 敏感信息泄露漏洞等。除“Juniper Junos 拒绝服务漏洞（CNVD-2017-00603、CNVD-2017-00604）”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-2017-00602
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00603
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00604
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00605
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00606

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00607

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00608

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00609

5、Apple Logic Pro X 和 GarageBand 存在内存破坏漏洞

Apple Logic Pro x 是苹果官方推出的一款音乐制作编辑软件；GarageBand 是苹果机器上的音乐演奏、合成、录制工具。本周，Apple 被披露存在内存破坏漏洞。攻击者可以利用该漏洞执行任意代码。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-2017-00665

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-2017-00187	Nagios 不完全修复本地权限提升漏洞	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/2016/q4/783
CNVD-2017-00455	多个 Samsung Android Mobile Phones 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://security.samsungmobile.com/smrupdate.html#SMR-JAN-2017
CNVD-2017-00483	GnuTLS 'lib/opencdk/read-packet.c'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://gnutls.org/security.html#GNUTLS-SA-2017-1
CNVD-2017-00487	libgit2 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/libgit2/libgit2
CNVD-2017-00489	libgit2 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/libgit2/libgit2
CNVD-2017-00507	Splunk Enterprise 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.splunk.com/view/SP-CAAAPSR
CNVD-2017-00555	Lenovo XClarity Administrator 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.lenovo.com/us/en/product_security/LEN_10605
CNVD-2017-00553	Advantech WebAccess 'updateTemplate.aspx' SQL 注入	高	用户可联系供应商获得补丁信息：http://www.advantech.com/

	漏洞		
CNVD-2017-00556	EllisLab CodeIgniter 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：https://github.com/bcit-ci/CodeIgniter/pull/4966
CNVD-2017-00560	Web Client SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.video-insight.com/
CNVD-2017-00581	Samsung Note 拒绝服务漏洞（CNVD-2017-00581）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://security.samsungmobile.com/smrupdate.html#SMR-JAN-2017

表 4 部分重要高危漏洞列表

小结：1 月 18 日，Oracle 发布了 2017 年 1 月份的安全更新，修复了其多款产品存在的 270 个安全漏洞。本次安全更新提供了有 252 个漏洞可被远程利用。此外，Google、IBM、Juniper Networks 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、泄露敏感信息或发起拒绝服务攻击等。另外，Apple 被披露存在内存破坏漏洞。攻击者可以利用该漏洞执行任意代码。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.利用漏洞窃取麦当劳网站注册用户密码

利用不安全的加密存储（Insecure_Cryptographic_Storage）漏洞和服务端反射型 XSS 漏洞，实现对麦当劳网站（McDonalds.com）注册用户的密码窃取，进一步测试，还可能获取到网站注册用户的更多信息。攻击者利用解密函数代码可以实现对客户端或双向加密存储的密码破解。对发现的被存储 Cookie 值 penc 进行解密。

参考链接：http://www.freebuf.com/vuls/125509.html

2. 利用钓鱼技术骗取 Gmail 用户账户

一种更加隐蔽有效的网络钓鱼技术，正试图骗取 Gmail 用户账户信息。它不仅针对那些普通用户，那些经验丰富的高级用户，也受到了不同程度的影响！一旦攻击者成功登陆到你的账户，他们就自动获取到了你所有邮件的访问接收及发放权限。攻击者还会利用密码重置机制，来修改你使用该邮箱绑定的其他一些服务密码。用于窃取 Gmail 上的用户名和密码的网络钓鱼攻击。这种技术不仅限于钓取 Gmail 账户信息，它还可以用于从许多其他平台窃取凭证。建议大家在进入一些关键性网站时，最好采用手动输入的方式，或通过搜索引擎查找有绿色官方验证标识的网站。同时，对一些重要的账户密码，进行定期的密码更换。

参考链接：http://www.freebuf.com/vuls/124864.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