

信息安全漏洞周报

2016 年 11 月 28 日-2016 年 12 月 04 日

2016 年第 49 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 200 个，其中高危漏洞 81 个、中危漏洞 109 个、低危漏洞 10 个。漏洞平均分为 6.42。本周收录的漏洞中，涉及 0day 漏洞 23 个（占 12%）。其中互联网上出现“Less Compiler 任意代码执行漏洞、EasyPHP Devserver 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 771 个，与上周（602 个）环比增长 22%。

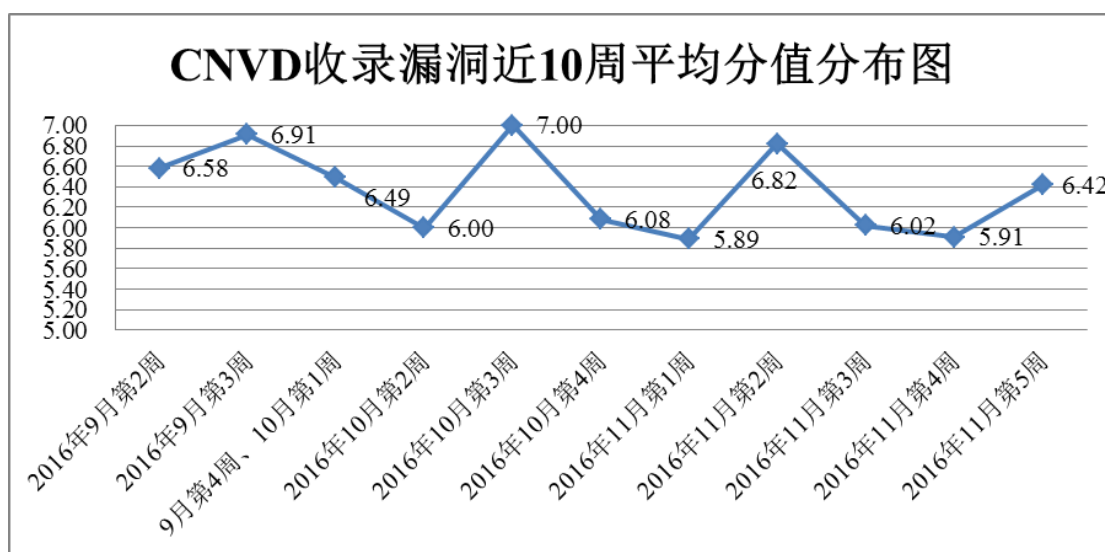


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 11 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 200 个漏洞。报送情况如表 1 所示。其中，天融信、恒安嘉新、杭州安恒信息技术有限公司、安天实验室等单位报送数量较多。360 网神、漏洞盒子、广州圣辉信息技术有限公司

司、江西安服信息产业有限公司及其他个人白帽子向 CNVD 提交了 771 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	559	559
天融信	196	0
恒安嘉新	120	0
杭州安恒信息技术有 限公司	84	0
安天实验室	60	0
中国电信集团系统集 成有限责任公司	55	0
H3C	49	0
启明星辰	9	9
北京数字观星科技有 限公司	5	0
西安四叶草信息技术 有限公司	1	1
南京铱迅信息技术股 份有限公司	1	1
漏洞盒子	96	96
广州圣辉信息技术有 限公司	2	2
江西安服信息产业有 限公司	1	1
上海云盾信息技术有 限公司	2	2
CNCERT 山西分中心	19	19
CNCERT 上海分中心	3	3
CNCERT 宁夏分中心	2	2
CNCERT 陕西分中心	1	1
CNCERT 江西分中心	1	1

个人	74	74
报送总计	1340	771
录入总计	200（去重）	771

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 200 个漏洞。其中应用程序漏洞 117 个，web 应用漏洞 50 个，操作系统漏洞 18 个，网络设备漏洞 14 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	117
web 应用漏洞	50
操作系统漏洞	18
网络设备漏洞	14
安全产品漏洞	1

表 2 漏洞按影响类型统计表

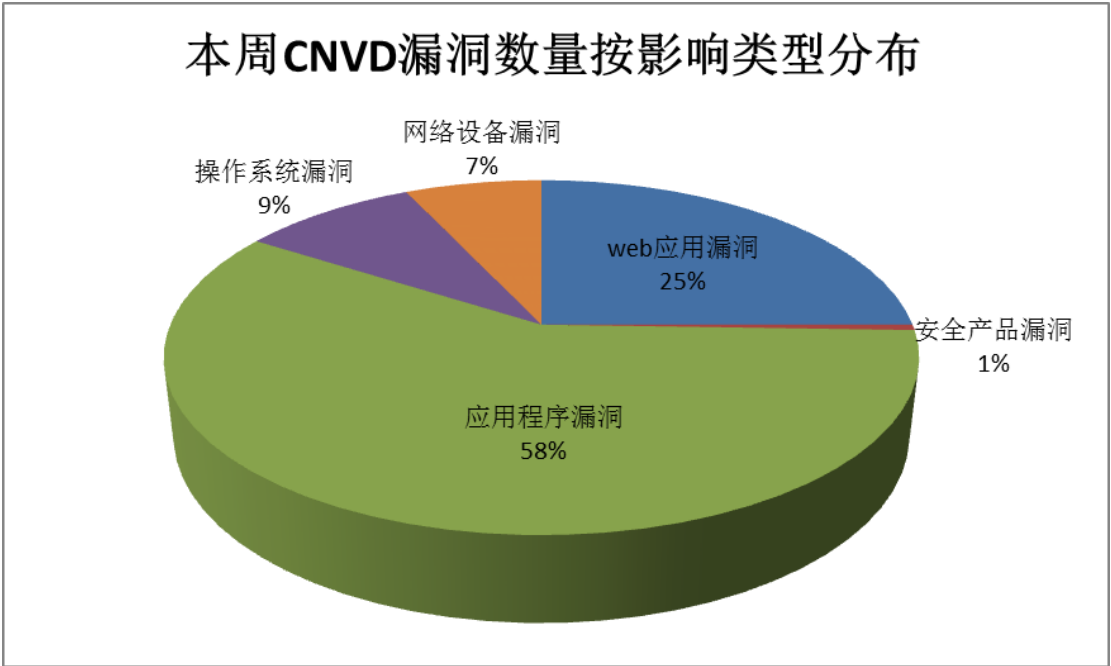


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 MyBB、w3m、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	MyBB	25	13%
2	w3m	24	12%

3	IBM	20	10%
4	Huawei	11	6%
5	Xen	10	5%
6	Apple	10	5%
7	Apache	7	3%
8	LibTIFF	5	3%
9	VMware	4	2%
10	其他	84	41%

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 6 个电信行业漏洞，12 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图所示）。其中，“多款华为交换机存在拒绝服务漏洞、IBM Tivoli Storage Manager FastBack 堆栈缓冲区溢出漏洞、Apache Tomcat 远程代码执行漏洞、Emerson DeltaV 提权漏洞、Siemens SIMATIC CP 343-1 Advanced devices 跨站请求伪造漏洞”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/>

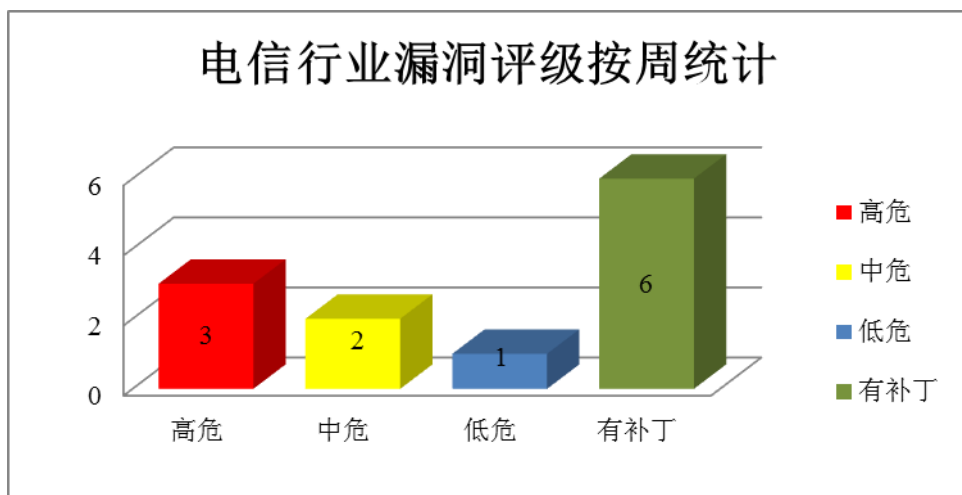


图 3 电信行业漏洞统计

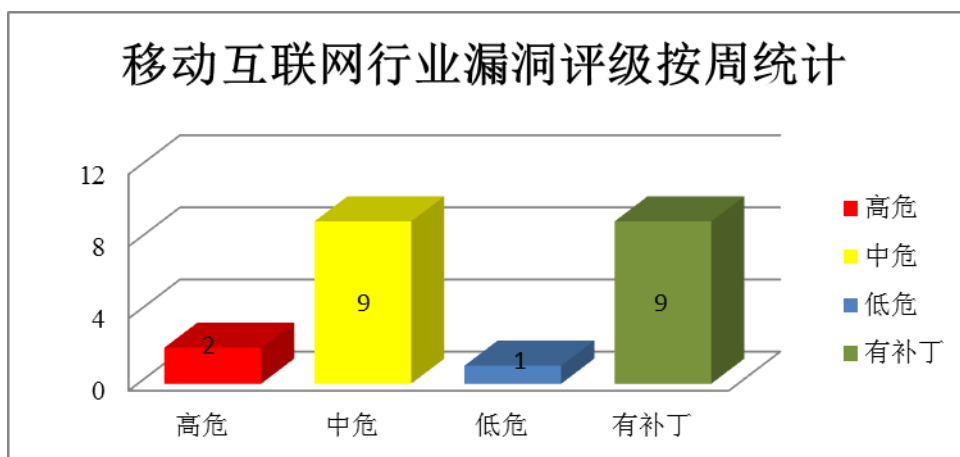


图 4 移动互联网行业漏洞统计

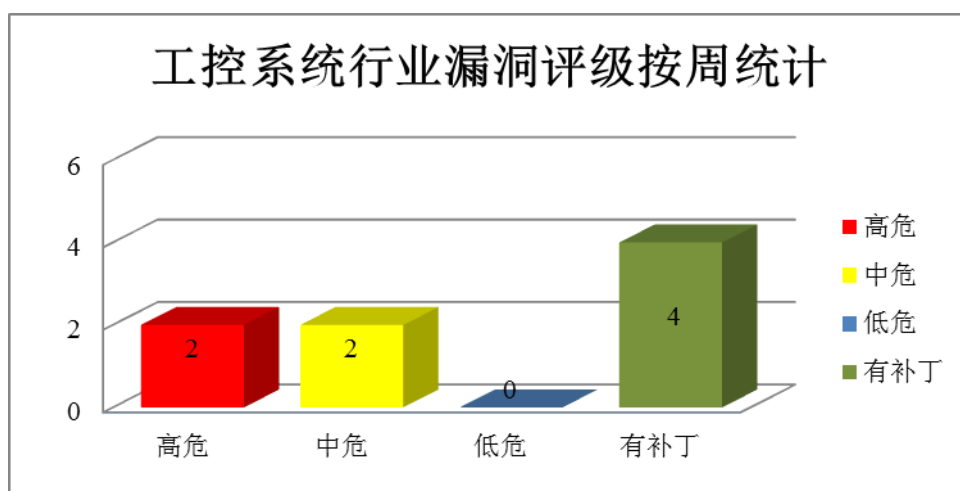


图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM iNotes 是美国 IBM 公司的一套基于 Web 的电子邮件软件；Domino 是一套用于托管社交商务应用的平台；IBM BigFix Remote Control 是一套远程控制系统。本周，上述产品被披露存在信息泄露和跨站脚本漏洞，攻击者可利用漏洞泄露敏感信息和进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：IBM iNotes 和 Domino 跨站脚本漏洞（CNVD-2016-11818、CNVD-2016-11819、CNVD-2016-11820、CNVD-2016-11821）、IBM BigFix Remote Control 信息泄露漏洞、IBM BigFix Remote Control 信息泄露漏洞（CNVD-2016-11744、CNVD-2016-11693、CNVD-2016-11814）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-2016-11818>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11819>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11820>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11821>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11694>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11744>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11693>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11814>

2、Apple 产品安全漏洞

Apple iOS 是美国苹果（Apple）公司为移动设备所开发的一套操作系统。Safari 是其中的一个 Web 浏览器组件。Apple macOS Sierra 是为 Mac 计算机所开发的一套专用操作系统。Core Image 是其中的一个图形过滤器框架。ImageIO 是其中的一个用来执行常见的图像 I/O 操作的静态方法。Mail 是其中的一个邮件模块。Apple WebKit 是开源的 web 浏览器引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、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 iOS Safari 拒绝服务漏洞、Apple macOS Sierra Core Image 内存破坏漏洞、Apple macOS Sierra ImageIO 任意代码执行漏洞、Apple macOS Sierra Mail 拒绝服务漏洞、Apple iOS 和 Apple macOS 信息泄露漏洞、Apple WebKit 存在多个内存破坏漏洞、Apple iOS and Mac OS 安全绕过漏洞（CNVD-2016-11549）、Apple iOS and Mac OS 安全绕过漏洞等。其中，“Apple macOS Sierra Core Image 内存破坏漏洞、Apple macOS Sierra ImageIO 任意代码执行漏洞、Apple WebKit 存在多个内存破坏漏洞”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-2016-11586>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11595>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11594>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11593>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11584>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11640>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11549>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11550>

3、Apache 产品安全漏洞

Apache Subversion 是美国阿帕奇（Apache）软件基金会的一套开源的版本控制系统；Karaf 是一个可以用于部署各种组件、应用程序的 OSGi 容器；Apache Hadoop 是一套开源的分布式系统基础架构；Apache Tomcat 是一个流行的开源 JSP 应用程序；Apache OpenOffice（OOo）是一款开源的办公软件套件。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、绕过安全限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apache Subversion 拒绝服务漏洞、Apache Karaf 远程代码执行漏洞、Apache Hadoop 任意命令执行漏洞、Apache Tomcat 远程代码执行漏洞、Apache Tomcat 拒绝服务漏洞（CNVD-2016-11592）、Apache Tomcat 安全限制绕过漏洞（CNVD-2016-11591）、Apache OpenOffice 非引用 Windows 搜索路径漏洞等。其中，“Apache Karaf 远程代码执行漏洞、Apache Tomcat 远程代码执行漏洞、Apache OpenOffice 非引用 Windows 搜索路径漏洞”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-2016-11813>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11769>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11748>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11583>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11592>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11591>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11590>

4、MyBB 产品安全漏洞

MyBB（又名 MyBulletinBoard）是 MyBB 团队开发的一套用 PHP 和 MySQL 开发的免费且基于 Web 的论坛软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞访问或修改数据、泄露敏感信息或绕过安全限制等。

CNVD 收录的相关漏洞包括：MyBB 存在多个漏洞（CNVD-2016-11600、CNVD-2016-11601、CNVD-2016-11602、CNVD-2016-11603、CNVD-2016-11604、CNVD-2016-11605、CNVD-2016-11606、CNVD-2016-11607）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-2016-11600>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11601>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11602>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11603>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11604>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11605>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11606>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11607>

5、OIC Exponent CMS SQL 注入漏洞（CNVD-2016-11771）

OIC Exponent CMS 是美国 OIC 集团公司的一套基于 PHP 的免费、开源的模块化内容管理系统 (CMS)。本周, OIC 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意 SQL 命令。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-2016-11771>

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-2016-11681	w3m 任意代码执行漏洞 (CNVD-2016-11681)	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://github.com/tats/w3m
CNVD-2016-11682	w3m 任意代码执行漏洞 (CNVD-2016-11682)	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://github.com/tats/w3m
CNVD-2016-11683	w3m 任意代码执行漏洞 (CNVD-2016-11683)	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://github.com/tats/w3m
CNVD-2016-11685	w3m 任意代码执行漏洞 (CNVD-2016-11685)	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://github.com/tats/w3m
CNVD-2016-11684	w3m 任意代码执行漏洞 (CNVD-2016-11684)	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://github.com/tats/w3m
CNVD-2016-11703	Xen 权限提升漏洞 (CNVD-2016-11703)	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://xenbits.xenproject.org/xsa/advisory-191.html
CNVD-2016-11704	Xen 权限提升漏洞 (CNVD-2016-11704)	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://xenbits.xenproject.org/xsa/advisory-198.html
CNVD-2016-11705	Xen 权限提升漏洞 (CNVD-2016-11705)	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://xenbits.xenproject.org/xsa/advisory-198.html
CNVD-201	Xen 内存破坏漏洞	高	目前厂商已经发布了升级补丁以修

6-11707			复此安全问题，补丁获取链接： http://xenbits.xenproject.org/xsa/advisory-195.html
CNVD-2016-11706	Xen 权限提升漏洞 (CNVD-2016-11706)	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://xenbits.xenproject.org/xsa/advisory-197.html

表 4 部分重要高危漏洞列表

小结：本周，IBM 产品被披露存在信息泄露和跨站脚本漏洞，攻击者可利用漏洞泄露敏感信息和发起跨站脚本攻击。此外，Apple、Apache、MyBB 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、执行任意代码、绕过安全限制或发起拒绝服务攻击等。另外，OIC 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意 SQL 命令。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. 黑客正在利用 Firefox 的 0day 漏洞攻击 Tor 用户

Tor 官网上首次出现了关于一个未知的 Firefox 0day 漏洞的消息。其中包含有数百行的漏洞利用代码 (JavaScript)，攻击者可以利用这份代码来攻击 Tor 浏览器的用户。安全研究专家在对代码进行了分析之后表示，攻击代码利用了一个内存崩溃漏洞，该漏洞将允许攻击者在运行了 Windows 操作系统的计算机中执行恶意代码。Mozilla 也建议用户如果用户仍然想使用 Firefox 的话，至少应该禁用访问网站的 JavaScript 脚本。除此之外，用户也应该停止使用 Tor。

参考链接：<http://www.freebuf.com/news/121892.html>

2. 超 100 万谷歌账户被黑，Android 恶意程序 Gooligan 正极速蔓延

一款新的 Android 恶意软件已经入侵了超过 100 万谷歌账户，还在以每日感染 13,000 个设备的速度蔓延。主要针对使用 Android 4.x(果冻豆和 KitKat)和 Android 5.x(棒棒糖)这两个系统版本的用户——目前市场上有 74% 的 Android 手机都仍在运行这两个版本的系统。这个叫做 Gooligan 的恶意软件可以植入到这些 Android 设备上，窃取设备上存储的谷歌账户和身份验证 token 信息。只要入侵者掌握了这些信息，他们就能劫持你的谷歌账号，从各类谷歌 App 中获取你的敏感信息。应该是有史以来最严重的谷歌账户被黑事件。据 Check Point 统计，这次被 Gooligan 恶意软件感染的重灾区就在亚洲。

参考链接：<http://www.freebuf.com/news/121685.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