

信息安全漏洞周报

2017 年 08 月 28 日-2017 年 09 月 03 日

2017 年第 36 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 348 个，其中高危漏洞 108 个、中危漏洞 215 个、低危漏洞 25 个。漏洞平均分为 5.94。本周收录的漏洞中，涉及 0day 漏洞 66 个（占 19%），其中互联网上出现“多款 ASUS 产品 Asuswrt-Merlin 固件栈缓冲区溢出漏洞”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 1641 个，与上周（1483 个）环比增长 11%。

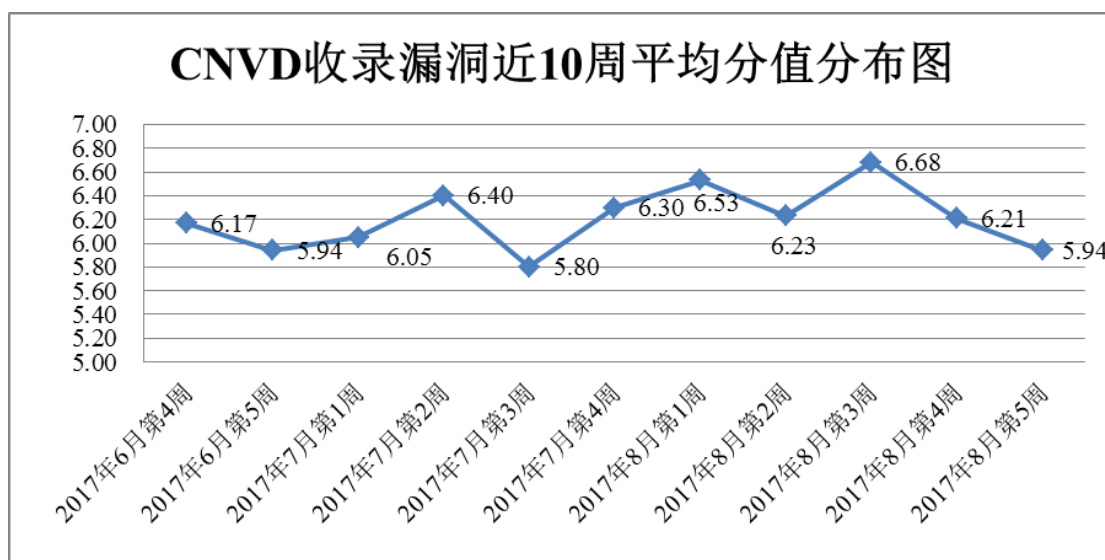


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 家成员单位、企业用户及个人用户报送了本周收录的全部 348 个漏洞。报送情况如表 1 所示。其中，安天实验室、H3C、华为技术有限公司、天融信、启明星辰等单位报送数量较多。四川虹微技术有限公司、深圳市鼎安天下信息科技有限公司、

上海犇众信息技术有限公司、江苏同袍信息科技有限公司、中新网络信息安全股份有限公司、中国航天科工集团第四研究院软件评测中心、北京安码科技有限公司、山石网科通信技术有限公司、广州万方计算机科技有限公司、北京市电子产品质量检测中心、广州软云计算机科技有限公司、杭州朔方信息技术有限公司、华讯方舟通信设备有限公司、西安尚易安华信息科技有限公司、邹平九零冰讯网络科技有限公司及其他个人白帽子向 CNVD 提交了 1641 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	283	283
安天实验室	213	1
H3C	204	0
华为技术有限公司	194	0
天融信	192	0
启明星辰	159	15
中国电信集团系统集成有 限责任公司	128	27
恒安嘉新	125	0
漏洞盒子	75	75
东软	72	3
北京数字观星科技有限公 司	62	0
绿盟科技	61	0
杭州安恒信息技术有限公 司	53	0
厦门服云信息科技有限公 司	15	1
广西鑫瀚科技有限公司	5	5
深圳市腾讯计算机系统有 限公司（玄武实验室）	4	4
四川虹微技术有限公司 （子午攻防实验室）	266	266
深圳市鼎安天下信息科技 有限公司	14	14

上海犇众信息技术有限公司	5	5
江苏同袍信息科技有限公司	5	5
中新网络信息安全股份有限公司	5	5
中国航天科工集团第四研究院软件评测中心（北京）	4	4
北京安码科技有限公司	3	3
山石网科通信技术有限公司	2	2
广州万方计算机科技有限公司	2	2
北京市电子产品质量检测中心	1	1
广州软云计算机科技有限公司	1	1
杭州朔方信息技术有限公司	1	1
华讯方舟通信设备有限公司	1	1
西安尚易安华信息科技有限公司	1	1
邹平九零冰讯网络科技有限公司	1	1
浙江分中心	3	3
宁夏分中心	1	1
陕西分中心	1	1
上海分中心	1	1
个人	909	909
报送总计	2644	1641
录入总计	248（去重）	1641

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 348 个漏洞。其中应用程序漏洞 247 个，web 应用漏洞 36 个，操作系统漏洞 30 个，网络设备漏洞 25 个，安全产品漏洞 6 个，数据库漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	247
web 应用漏洞	36
操作系统漏洞	30
网络设备漏洞	25
安全产品漏洞	6
数据库漏洞	4

表 2 漏洞按影响类型统计表

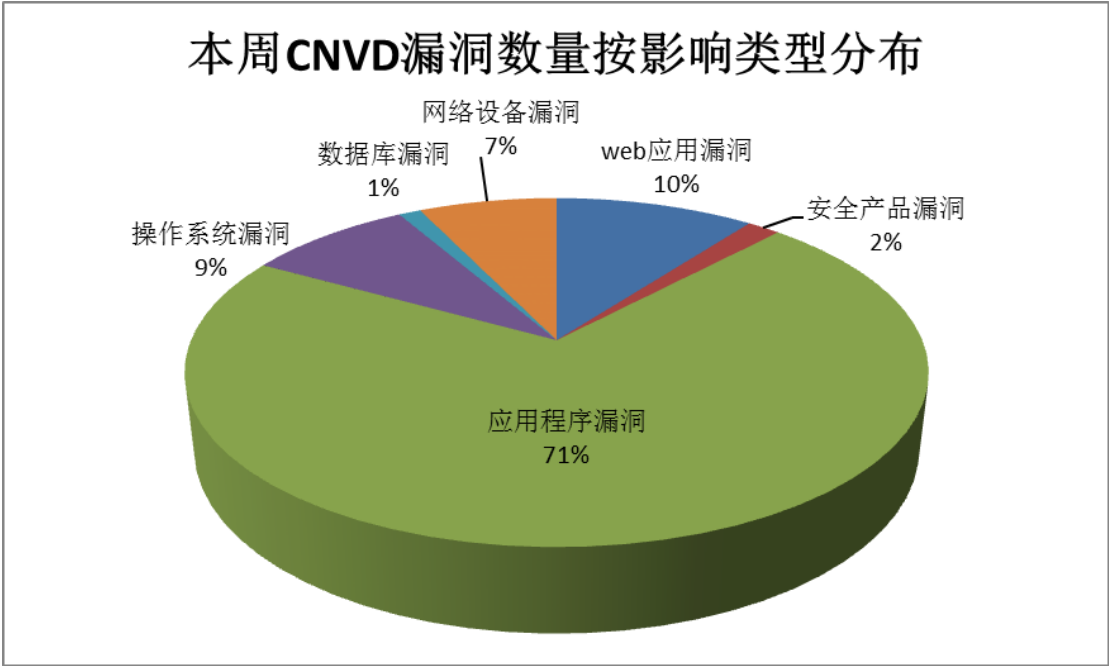


图 2 本周漏洞按影响类型分布

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	33	9%
2	Oracle	25	7%
3	IBM	18	5%
4	Microsoft	16	5%
5	OpenCV	13	4%
6	ImageMagick	11	3%
7	Advantech	9	3%
8	Linux	9	3%

9	Fiyo	9	3%
10	其他	205	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 15 个电信行业漏洞，52 个移动互联网行业漏洞，23 个工控系统行业漏洞（如下图所示）。其中，“多款 Juniper 产品 Junos OS 权限提升漏洞、D-Link DIR 权限提升漏洞、Android Media framework libavc 拒绝服务漏洞、Advantech Web Access 权限提升漏洞、Moxa SoftCMS Live Viewer SQL 注入漏洞”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/>

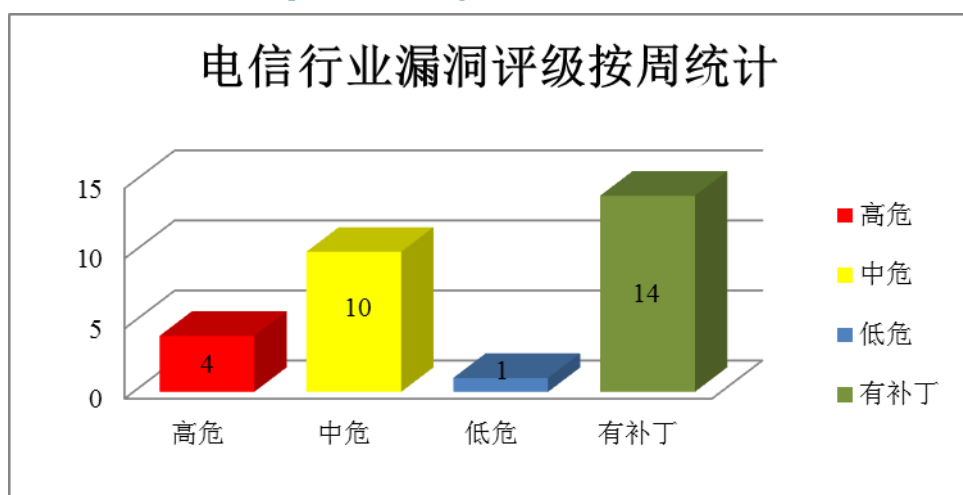


图 3 电信行业漏洞统计

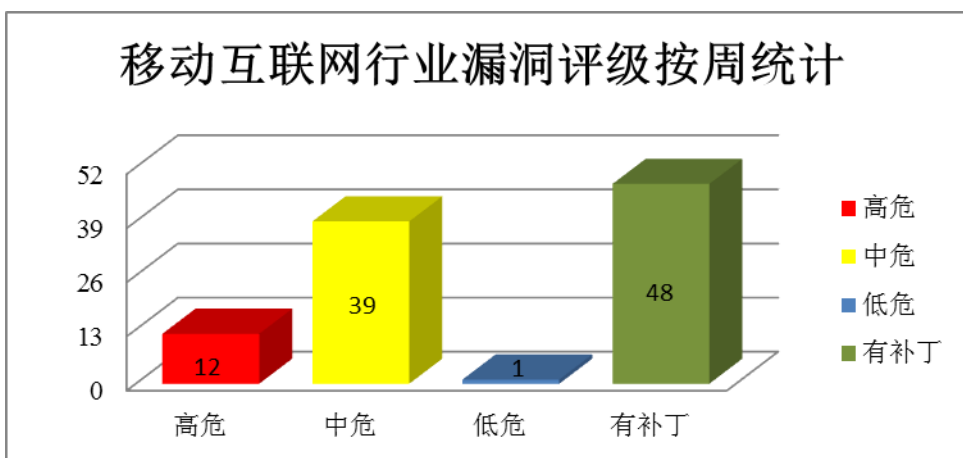


图 4 移动互联网行业漏洞统计

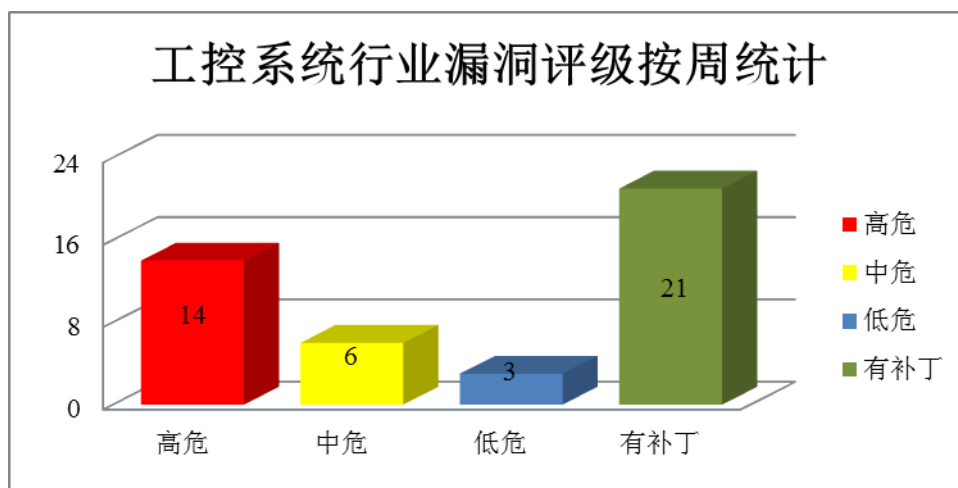


图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌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。本周，上述产品被披露存在拒绝服务和远程代码执行漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Android Media framework avc decoder 远程代码执行漏洞、Android Media framework h263 decoder 远程代码执行漏洞、Android Media framework libavc 拒绝服务漏洞、Android Media framework libavc 远程代码执行漏洞、Android Media framework libavc 远程代码执行漏洞（CNVD-2017-23413）、Android Media framework libhevc 远程代码执行漏洞、Android Media framework libmpeg2 远程代码执行漏洞、Android Media framework mpeg2 decoder 远程代码执行漏洞。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-2017-23420>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23411>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23405>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23410>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23413>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23432>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23431>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23412>

2、Microsoft 产品安全漏洞

Microsoft Windows 10 是美国微软公司发布的一套新一代跨平台操作系统。Microsoft Edge 是其中的一款系统附带的 Web 浏览器。JavaScript engines 是其中的一个 JavaScript 引擎组件。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意的代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Edge 内存破坏漏洞（CNVD-2017-24167、CNVD-2017-24168、CNVD-2017-24169、CNVD-2017-24170）、Microsoft Windows Edge JavaScript 引擎远程代码执行漏洞（CNVD-2017-23797、CNVD-2017-23798、CNVD-2017-23799、CNVD-2017-23800）。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-2017-24167>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24168>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24169>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24170>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23797>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23798>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23799>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23800>

3、Advantech 产品安全漏洞

Advantech WebAccess 是研华（Advantech）公司的一套基于浏览器架构的 HMI/SCADA 软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证、执行任意代码或提升权限等。

CNVD 收录的相关漏洞包括：Advantech WebAccess HEAP 缓冲区溢出漏洞、Advantech WebAccess 堆栈缓冲区溢出漏洞、Advantech WebAccess 缓冲区溢出漏洞（CNVD-2017-23885）、Advantech WebAccess 权限提升漏洞、Advantech WebAccess 未授权操作漏洞、Advantech WebAccess 验证绕过漏洞、Advantech WebAccess 任意代码执行漏洞（CNVD-2017-23882、CNVD-2017-23878）。除“Advantech WebAccess 任意代码执行漏洞（CNVD-2017-23878）”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-2017-23883>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23884>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23885>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23879>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23880>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23881>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23882>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-23878>

4、Oracle 产品安全漏洞

Oracle Financial Services Applications 是美国甲骨文（Oracle）公司的一套集核心银行、网上银行和财产管理于一身的金融服务软件。Oracle Sun Systems Products Suite 是一款 Sun 系统产品套件。Oracle Fusion Middleware 是一套面向企业和云环境的业务创新平台。Oracle WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。Outside In Technology 是其中的一个软件开发工具包组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的可用性、保密性和完整性。

CNVD 收录的相关漏洞包括：Oracle FLEXCUBE Private Banking 未授权读取漏洞、Oracle FLEXCUBE Private Banking 未授权访问漏洞、Oracle FLEXCUBE Universal Banking 未授权操作漏洞（CNVD-2017-24334、CNVD-2017-24342）、Oracle Outside In Technology 远程漏洞（CNVD-2017-24347、CNVD-2017-24348）、Oracle Solaris 远程漏洞（CNVD-2017-24337）、Oracle WebLogic Server 远程漏洞（CNVD-2017-24344）。其中，“Oracle Solaris 远程漏洞（CNVD-2017-24337）、Oracle WebLogic Server 远程漏洞（CNVD-2017-24344）”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-2017-24332>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24333>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24334>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24342>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24347>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24348>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24337>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-24344>

5、Siemens LOGO!8 BM 中间人攻击漏洞

LOGO!8 是西门子第 8 代智能逻辑控制器。本周，Siemens 被披露存在中间人攻击漏洞，攻击者可利用漏洞解密或修改网络流量。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-2017-24121>

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-2017-23305	Irssi 拒绝服务漏洞（CNVD-2017-23305）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://irssi.org/security/irssi_sa_2017_07.txt
CNVD-2017-23466	多款 EMC 产品不安全默认密码漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.emc.com/
CNVD-2017-23480	Apache OpenMeetings XML 外部实体注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://openmeetings.apache.org/
CNVD-2017-23873	SAP GRC 远程代码注入漏洞	高	用户可联系供应商获得补丁信息： https://www.sap.com/index.html
CNVD-2017-23959	FileCapsule Deluxe Portable 不安全动态加载漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.resume-next.com/
CNVD-2017-24122	Siemens LOGO!8 BM 会话 ID 泄露漏洞	高	用户可联系供应商获得补丁信息： https://www.siemens.com
CNVD-2017-24387	baserCMS SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://basercms.net/security/JVN78151490
CNVD-2017-24396	Juniper Junos 本地缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://kb.juniper.net/JSA10792
CNVD-2017-24398	LogicalDoc CommunityEdition 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://blog.logicaldoc.com/
CNVD-2017-24403	BUFFALO WAPM-1166D 和 WAPM-APG600H 身份验证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://buffalo.jp/support_s/s20170718.html

表 4 部分重要高危漏洞列表

小结：本周，Google 被披露存在拒绝服务和远程代码执行漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。此外，Microsoft、Advantech、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，Siemens 被披露存在中间人攻击漏洞，攻击者可利用漏洞解密或修改网络流量。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. 大量 IoT 设备 Telnet 密码列表遭泄露

一份包含几千条 telnet 密码的列表自 7 月 11 日起被贴到了 Pastebin 上，这些密码可

以被黑客用来扩大僵尸网络。安全研究员 Ankit Anubhav 发现，这份列表中包含了 IP 地址、设备名称和 telnet 密码，列表中大部分的用户名密码组合都是” admin:admin” 或者” root:root” 等。这整份列表中包含 143 种密码组合，其中 60 种密码组合都来自于 Mirai Telnet 扫描器。通过 telnet，黑客可以轻松攻占主机，进而扩大僵尸网络，如果要进行 DDoS 攻击，其影响也会更大。研究人员表示，列表里仍可以访问的 IP 中，大部分(61%)都位于中国。大部分仍在响应的 IP 都属于路由器。

参考链接: <http://www.freebuf.com/news/145739.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