

信息安全漏洞周报

2015 年 05 月 25 日-2015 年 05 月 31 日

2015 年第 22 期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为**低**。

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 152 个，其中高危漏洞 56 个、中危漏洞 88 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 134 个。本周收录的漏洞中，已有 117 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“WordPress Simple Backup 插件'tools.php'任意文件下载漏洞”、“Forma Lms SQL 注入漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 7 家成员单位、合作伙伴及个人报送了本周收录的全部 152 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、启明星辰、天融信等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、**北京国舜科技有限公司**、深圳市深信服电子科技有限公司、四川大学信息安全研究所及白帽子向 CNVD 提交了 732 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
奇虎	376	376
安天实验室	151	0
启明星辰	115	0
天融信	96	11
绿盟科技	23	0

知道创宇	22	0
恒安嘉新	14	0
乌云	290	290
漏洞盒子	4	4
北京国舜科技有限公司	1	1
深圳市深信服电子科技有限公司	1	1
四川大学信息安全研究所	1	1
CNCERT 江西分中心	4	4
CNCERT 河南分中心	1	1
个人	43	43
报送总计	1142	732
录入总计	152（去重）	732

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、IBM、WordPress 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Google	16	11%
2	IBM	11	7%
3	WordPress	10	7%
4	SAP	9	6%
5	Moodle	7	5%
6	Drupal	6	4%
7	Cisco	6	4%
8	HP	3	2%
9	ZTE	2	1%
10	其他	82	53%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周, CNVD 收录了 152 个漏洞。其中应用程序漏洞 105 个, WEB 应用漏洞 32 个, 网络设备漏洞 6 个, 数据库漏洞 5 个, 操作系统漏洞 2 个, 安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	105
WEB 应用漏洞	32
网络设备漏洞	6
数据库漏洞	5
操作系统漏洞	2
安全产品漏洞	2

表 3 漏洞按影响类型统计表

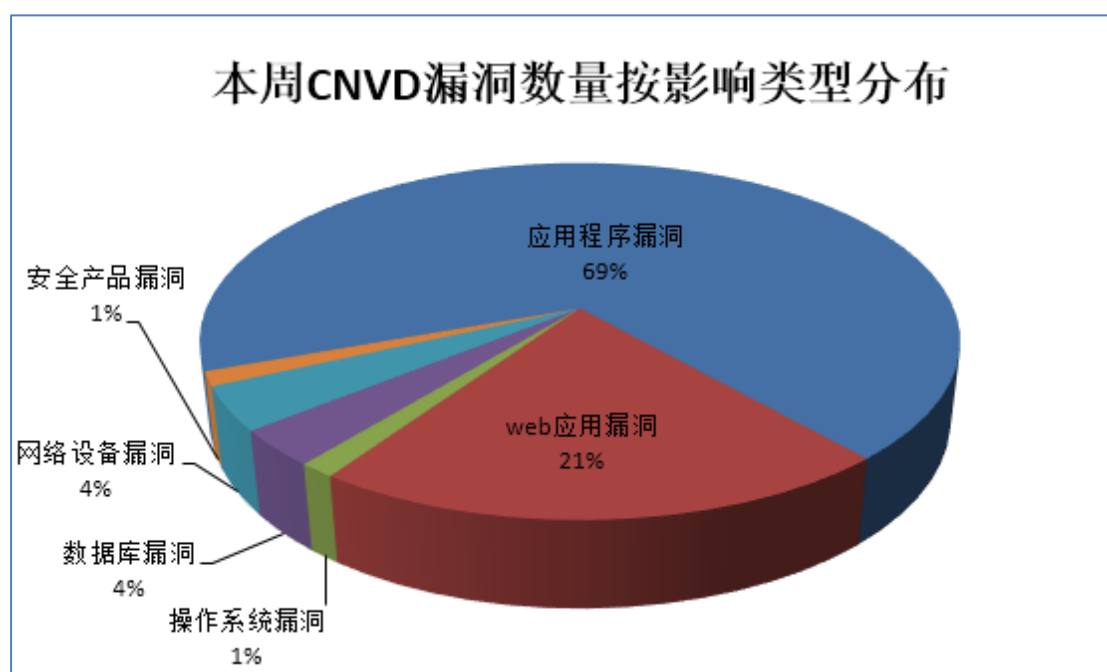


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周, CNVD 收录了 10 个电信行业漏洞, 2 个移动互联网行业, 2 个工控系统行业漏洞 (如下图表所示)。其中, “MAS 中国移动代理服务器 SQL 注入漏洞、SAP AfariaXComms Process 远程缓冲区溢出漏洞” 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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-03364	IBM WebSphere MQ 拒绝服务漏洞 (C	低	是

		NVD-2015-03364)		
电信	CNVD-2015-03377	MAS 中国移动代理服务器 SQL 注入漏洞	高	是
电信	CNVD-2015-03403	Cisco Prime Central for Hosted Collaboration Solution 跨站请求伪造漏洞	中	是
电信	CNVD-2015-03436	PostgreSQLpgcrypto 拒绝服务漏洞	中	是
电信	CNVD-2015-03446	IBM License Metric Tool 和 Endpoint Manager for Software Use Analysis 跨站请求伪造漏洞	中	是
电信	CNVD-2015-03452	IBM License Metric Tool 和 Endpoint Manager for Software Use Analysis 点击劫持漏洞	中	是
电信	CNVD-2015-03455	SolarWinds Network Performance Monitor 'ReturnUrl'开放重定向漏洞	中	否
电信	CNVD-2015-03461	PostgreSQL 'snprintf()'信息泄露漏洞	中	是
电信	CNVD-2015-03465	PostgreSQL 远程拒绝服务漏洞	中	是
电信	CNVD-2015-03471	Cisco Unified Communications Manager 存在多个漏洞	中	是
移动互联网	CNVD-2015-03413	SAP AfariaXComms Process 远程缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-03409	SAP Afaria 身份验证绕过漏洞	中	是
工控系统	CNVD-2015-03338	PeakHMI HMI 存在未明远程拒绝服务漏洞	中	否
工控系统	CNVD-2015-03341	Infilink HMI 存在未明远程拒绝服务漏洞	中	否

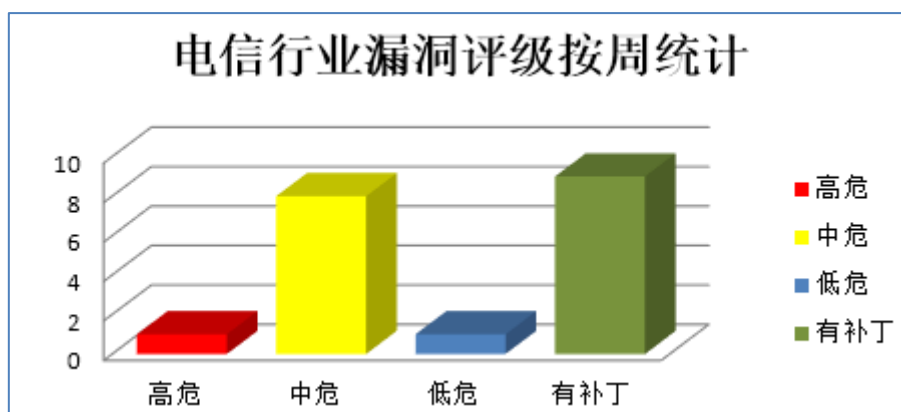


图 1 电信行业漏洞统计

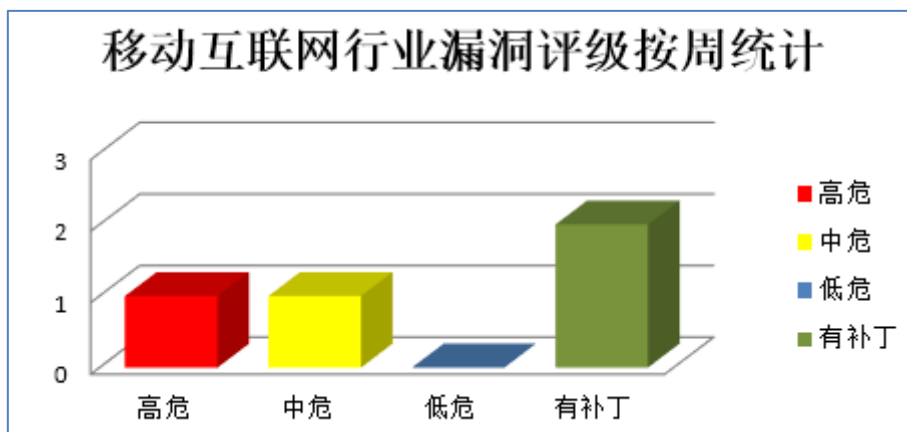


图 2 移动互联网行业漏洞统计

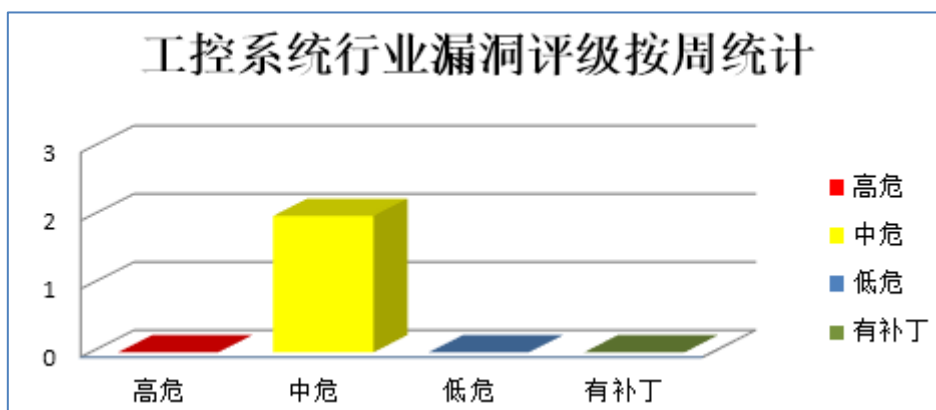


图 3 工控系统行业漏洞统计

本周重要漏洞信息

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

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。本周，上述产品被披露存在拒绝服务、内存错误引用、缓冲区溢出和代码注入漏洞。攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome--size-limit value 拒绝服务漏洞、Google Chrome Blink 缓冲区溢出漏洞、Google Chrome Blink SVG 内存错误引用漏洞、Google Chrome 缓冲区溢出漏洞（CNVD-2015-03355）、Google Chrome Blink 代码注入漏洞、Google Chrome WebRTC 内存错误引用漏洞、Google Chrome PDFium 代码注入漏洞、Google Chrome 拒绝服务漏洞（CNVD-2015-03372）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2015-03349>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03350>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03351>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03355>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03347>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03348>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03372>

2、SAP 产品安全漏洞

SAP 为“Systems Applications and Products in Data Processing”的简称,是 SAP 公司的产品——企业管理解决方案的软件名称。SAP NetWeaver 是 SAP 的软件的基础平台,分为 SAP Netweaver JAVA 和 Netweaver ABAP,其前身是 SAP BASIS 组件.因为互联网和 JAVA 的发展,SAP 调整了基础平台的架构,加入对 JAVA 的支持,同时也增强了网络应用,并更名为 SAP Netweaver。SAP Sybase Adaptive Server Enterprise 是一套关系型数据库管理系统。SAP HANA 是一套高性能的实时数据分析平台,它提供数据查询功能,用户可直接对大量实时业务数据进行查询和分析。SAP HANA Web-based Development Workbench 是一个基于 Web 的开发平台。SAP Content Server 是一款用来存储任何格式和内容的电子文档服务器。本周,上述产品被披露存在缓冲区溢出、拒绝服务、外部实体、SQL 注入和验证绕过漏洞。攻击者可利用漏洞获取敏感信息,提升权限、执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括: SAP AfariaXcomms 进程缓冲区溢出漏洞、SAP Sybase Adaptive Server Enterprise SQL 注入漏洞、SAP HANA Web-based Development Workbench SQL 注入漏洞、SAP AfariaXComms Process 远程缓冲区溢出漏洞、SAP NetWeaver AS Java XML 外部实体漏洞、SAP Afaria 身份验证绕过漏洞、SAP Content Server 存在未明拒绝服务漏洞。其中,除“SAP NetWeaver AS Java XML 外部实体漏洞、SAP Afaria 身份验证绕过漏洞、SAP Content Server 存在未明拒绝服务漏洞”外,其余漏洞的综合评级均为“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-2015-03477>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03410>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03411>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03413>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03478>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03409>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03412>

3、IBM 产品安全漏洞

IBM Security SiteProtector System 是一套可统一管理和分析网络、服务器和终端安全性代理及设备的集中式管理系统。IBM License Metric Tool 是一套可帮助 IBM Passport Advantage 客户决定其处理器价值单元 (PVU) 许可需求的免费工具；IBM Endpoint Manager for Software Use Analysis 是一套通过精确发现所有设备中的软件是否经过授权从而实现整体的软件资产管理的解决方案。IBM Curam Social Program Management 是一套社会计划管理解决方案。该方案支持终端到终端社会项目交付的过程。IBM Domino 是美国 IBM 公司的集电子邮件、文档数据库、快速应用开发技术以及 Web 技术为一体的电子邮件与群集平台。本周，上述产品被披露存在多个安全漏洞。攻击者可利用漏洞获取敏感信息、进行跨站请求伪造和跨站脚本攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Security SiteProtector System 目录遍历漏洞、IBM License Metric Tool 和 Endpoint Manager for Software Use Analysis 点击劫持漏洞、IBM Security SiteProtector System SQL 注入漏洞、IBM License Metric Tool 和 Endpoint Manager for Software Use Analysis 跨站请求伪造漏洞、IBM Curam Social Program Management 跨站脚本漏洞、IBM License Metric Tool 目录遍历漏洞、IBM Domino 堆栈缓冲区溢出漏洞 (CNVD-2015-03370、CNVD-2015-03370)。其中，“IBM Domino 堆栈缓冲区溢出漏洞 (CNVD-2015-03370、CNVD-2015-03370)”的综合评级均为“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-2015-03454>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03452>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03445>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03446>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03448>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03363>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03370>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03371>

4、Drupal 产品安全漏洞

Drupal 是一套用 PHP 语言开发的免费、开源的内容管理系统。本周，上述产品被披露存在信息泄露、跨站脚本、安全绕过和远程代码执行漏洞。攻击者可利用漏洞获取敏感信息、绕过安全限制、进行跨站攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Drupal Shipwire 模块跨站脚本漏洞、Drupal pass2pdf 模块信息泄露漏洞、Drupal Hostmaster 模块远程代码执行漏洞、Drupal Navigate 模块跨站脚本漏洞、Drupal Web Links 模块跨站脚本漏洞、Drupal Navigate 模块安全绕过漏洞。其中“Drupal Hostmaster 模块远程代码执行漏洞”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-2015-03392>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03393>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03394>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03398>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03395>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03397>

5、ZTE AC3633R 任意代码执行漏洞

ZTE AC3633R 是中兴通讯公司的一款无线调制解调器产品。本周，ZTE AC3633R 被披露存在综合评级为“高危”的任意代码执行漏洞。攻击者利用该漏洞可执行任意代码。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-2015-03408>

更多高危漏洞如表 3 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-2015-03316	Moodle 已封用户登录漏洞	高	Moodle 2.6.11, 2.7.8, 2.8.6, 2.9 已经修复该漏洞，建议用户下载更新： https://moodle.org
CNVD-2015-03318	Moodle 私有文件上传漏洞	高	Moodle 2.6.11, 2.7.8, 2.8.6, 2.9 已经修复该漏洞，建议用户下载更新： https://moodle.org
CNVD-2015-03322	NHN PlayArt LINE 远程代码执行漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://official-blog.line.me/ja/archives/24809761.html
CNVD-2015-03323	t1utils 缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.lcdf.org/~eddietwo/type/#t1utils
CNVD-2015-03325	Volition Pure Faction 栈缓冲区溢出漏洞	高	暂无
CNVD-2015-03327	Composer 远程代码执行漏洞	高	暂无
CNVD-2015-03329	HP LoadRunner 远程缓冲区溢出漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时

			下载更新： https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04594015
CNVD-2015-03337	Brainworks Software XpanceNET /index.php/request_passwordChange SQL 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://www.brainworks.com/
CNVD-2015-03336	Hue /usr/lib/hue/build/env/bin/supervisor 不安全权限设置漏洞	高	暂无
CNVD-2015-03366	KCodesNetUSB module for Linux kernel 堆栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： http://www.kcodes.com

表 3 部分高危漏洞列表

小结：本周，Google Chrome 被披露存在拒绝服务、内存错误引用、缓冲区溢出和代码注入漏洞。攻击者可利用漏洞发起拒绝服务攻击。此外，SAP、IBM、Drupal 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、提升权限、进行跨站脚本和跨站请求伪造攻击、发起拒绝服务攻击或者执行任意代码。另外，ZTE AC3633R 被披露存在一个高危零日漏洞，攻击者利用该漏洞可执行任意代码。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Apple 修补 Safari 产品漏洞

Safari 是苹果计算机的最新操作系统 Mac OS X 中的浏览器。

本周，Apple 修补了上述产品存在的远程拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/58965>

本周要闻速递

1. Android 手机恢复出厂设置后，数据依然可恢复

Android 恢复出厂设置功能有一个漏洞，即使你恢复了出厂设置，黑客依然可以恢复你的登录密码、短信、邮件和图片。剑桥大学的计算机研究员们对 5 个不同厂商的 Android 手机，发现超过五亿 Android 手机在恢复出厂设置后并没有完全擦除手机数据。

“恢复出厂设置”功能是 Android 手机系统内置的功能，这被认为是在出售、回收手机时最重要的功能，用以擦除手机上的所有机密信息。但是，计算机研究人员发现，即使

用户开启了全盘加密功能，数据还是可能会被恢复。研究人员从二手市场淘来 5 部不同厂商的手机，根据他们的估计，超过五亿智能手机不能够有效地擦除密码和其他敏感数据。另外，约 6.3 亿的设备不能擦除存放图片、视频等多媒体文件的外置 SD 卡。

参考链接：<http://www.freebuf.com/news/68268.html>

2. Linux/Moose 蠕虫：操纵路由器“帮你玩”社交网络

ESET 的安全研究员发表了一篇技术报告，报告中详细分析了一个新的蠕虫 Linux/Moose。它的攻击对象主要是调制解调器、家用路由器和其他嵌入式计算机，可将这些设备变成一个代理网络，然后创建伪造的社交账号实施欺诈行为。该恶意程序是由 Olivier Bilodeau 和 Thomas Dupuy 发现的，它会感染基于 Linux 的路由器和其他基于 Linux 系统的设备。如果它发现有其他的恶意程序和它争夺路由器的有限资源，会将其清除，然后继续寻找下一个感染目标。Moose 蠕虫不会利用路由器上存在的任何漏洞，它只会攻击那些配置较低并且还使用弱密码登录凭证的设备。这也意味着不仅仅是路由器会感染这种蠕虫，其他的设备也可能会感染，甚至是医疗设备。当然最受影响设备还是路由器，涉及的路由器品牌有：Actiontec、Hik Vision、Netgear、Synology、TP-Link、ZyXEL 和 Zhone。

参考链接：<http://www.freebuf.com/news/68580.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