

信息安全漏洞周报

2015 年 06 月 29 日-2015 年 07 月 05 日

2015 年第 27 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 167 个，其中高危漏洞 42 个、中危漏洞 109 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 153 个。本周收录的漏洞中，已有 129 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“LivelyCart SQL 注入漏洞”、“ZvingSoft SQL 注入漏洞”等零日攻击代码，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 6 家成员单位、合作伙伴及个人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，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、四川大学信息安全研究所、上海天泰网络技术有限公司、东莞市临渊信息技术有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 602 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	319	319
启明星辰	152	0
安天实验室	90	0
天融信	88	0
恒安嘉新	59	0

绿盟科技	23	0
乌云	229	229
漏洞盒子	28	28
四川大学信息安全研究所	3	3
上海天泰网络技术有限公司	1	1
东莞市临渊信息技术有限公司	1	1
CNCERT 山西分中心	6	6
CNCERT 甘肃分中心	4	4
CNCERT 福建分中心	3	3
个人	8	8
报送总计	1014	602
录入总计	167（去重）	602

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、Cisco、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	IBM	36	22%
2	Cisco	22	13%
3	WordPress	12	7%
4	Drupal	7	4%
5	Google	4	2%
6	ZOHO	4	2%
7	EMC	3	2%
8	SAP	3	2%
9	Synology	2	1%
10	其他	74	45%

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 167 个漏洞。其中应用程序漏洞 99 个，WEB 应用漏洞 40 个，网络设备漏洞 24 个，安全产品漏洞 2 个，操作系统漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	99
WEB 应用漏洞	40
网络设备漏洞	24
安全产品漏洞	2
操作系统漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

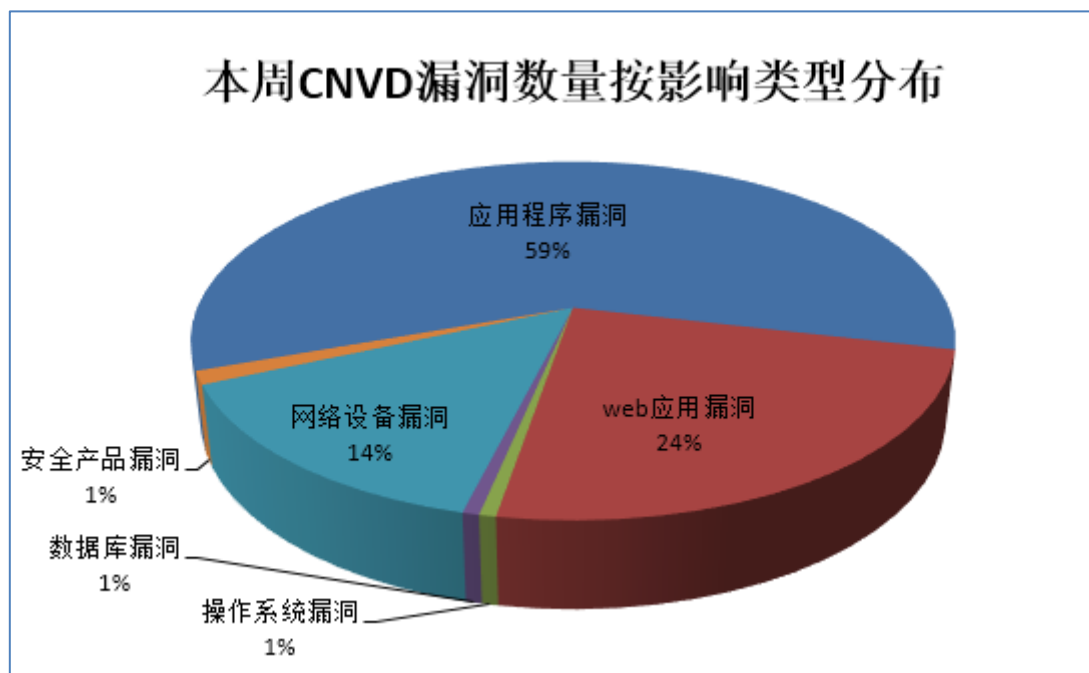


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 35 个电信行业漏洞，1 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图表所示）。其中，“Cisco AnyConnect Secure Mobility Client 权限设置漏洞、IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞（CNVD-2015-04168）、IBM Tivoli Storage Manager FastBack 任意命令执行漏洞（CNVD-2015-04165、CNVD-2015-04166、CNVD-2015-04167）、IBM Tivoli Storage Manager FastBack 任意文件读取漏洞（CNVD-2015-04163、CNVD-2015-04164）、IBM Tivoli Storage Manager FastBack 栈缓冲区

溢出漏洞（CNVD-2015-04169、CNVD-2015-04170、CNVD-2015-04171、CNVD-2015-04172、CNVD-2015-04173、CNVD-2015-04174、CNVD-2015-04175、CNVD-2015-04176、CNVD-2015-04177、CNVD-2015-04187、CNVD-2015-04188）、IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞（CNVD-2015-04168）”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-2015-04053	Huawei E5756S 身份验证绕过漏洞	中	是
电信	CNVD-2015-04038	Cisco AnyConnect Secure Mobility Client 权限设置漏洞	高	是
电信	CNVD-2015-04058	Alcatel-Lucent CellPipe 7130 RG 5Ae.M2013 HOL 跨站请求伪造漏洞	中	否
电信	CNVD-2015-04075	GarrettCom Magnum 6K 和 10K Switches 信息泄露漏洞	中	是
电信	CNVD-2015-04082	Cisco IOS XR 拒绝服务漏洞（CNVD-2015-04082）	中	是
电信	CNVD-2015-04080	Cisco Unified Presence Server 跨站脚本漏洞	中	是
电信	CNVD-2015-04090	GarrettCom Magnum 6K 和 10K Switches 本地安全绕过漏洞	低	是
电信	CNVD-2015-04091	GarrettCom Magnum 6K 和 10K Switches 远程拒绝服务漏洞	中	是
电信	CNVD-2015-04092	GarrettCom Magnum 6K 和 10K Switches 跨站脚本漏洞	中	是
电信	CNVD-2015-04116	Cisco IOS Software UBR Devices IPv6 VPN 拒绝服务漏洞	中	是
电信	CNVD-2015-04119	Cisco uBR10000 IOS 拒绝服务漏洞	中	是
电信	CNVD-2015-04150	Cisco Nexus 9000 Application Policy Infrastructure Controller 未授权访问漏洞	中	是
电信	CNVD-2015-04181	IBM WebSphere Commerce CRLF 注入漏洞	中	是
电信	CNVD-2015-04167	IBM Tivoli Storage Manager FastBack 任意命令执行漏洞（CNVD-2015-04167）	高	是
电信	CNVD-2015-04173	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2015-04173）	高	是
电信	CNVD-2015-04166	IBM Tivoli Storage Manager FastBack 任意命令执行漏洞（CNVD-2015-04166）	高	是
电信	CNVD-2015-04165	IBM Tivoli Storage Manager FastBack 任意命令执行漏洞（CNVD-2015-04165）	高	是
电信	CNVD-2015-04172	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2015-04172）	高	是

电信	CNVD-2015-04164	IBM Tivoli Storage Manager FastBack 任意文件读取漏洞 (CNVD-2015-04164)	高	是
电信	CNVD-2015-04163	IBM Tivoli Storage Manager FastBack 任意文件读取漏洞 (CNVD-2015-04163)	高	是
电信	CNVD-2015-04171	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04171)	高	是
电信	CNVD-2015-04170	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04170)	高	是
电信	CNVD-2015-04169	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04169)	高	是
电信	CNVD-2015-04168	IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞 (CNVD-2015-04168)	高	是
电信	CNVD-2015-04174	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04174)	高	是
电信	CNVD-2015-04176	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04176)	高	是
电信	CNVD-2015-04175	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04175)	高	是
电信	CNVD-2015-04177	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04177)	高	是
电信	CNVD-2015-04197	Samsung Galaxy S5 远程代码执行漏洞	高	否
电信	CNVD-2015-04202	Cisco Nexus 设备 Python 子系统本地权限提升漏洞	中	是
电信	CNVD-2015-04196	Cisco Nexus 设备 NS-OS 软件命令行解释器本地权限提升漏洞	中	是
电信	CNVD-2015-04188	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04188)	高	是
电信	CNVD-2015-04187	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-04187)	高	是
电信	CNVD-2015-04190	Cisco IOS Software UBR Devices IPv6 to IPv4 子系统竞争条件漏洞	中	是
电信	CNVD-2015-04216	IBM WebSphere MQ 信息泄露漏洞	中	是
移动互联网	CNVD-2015-04185	Android Droidware UK Explorer+ File Manager 应用程序目录遍历漏洞	中	是
工控系统	CNVD-2015-04191	PACTware 拒绝服务漏洞	低	是

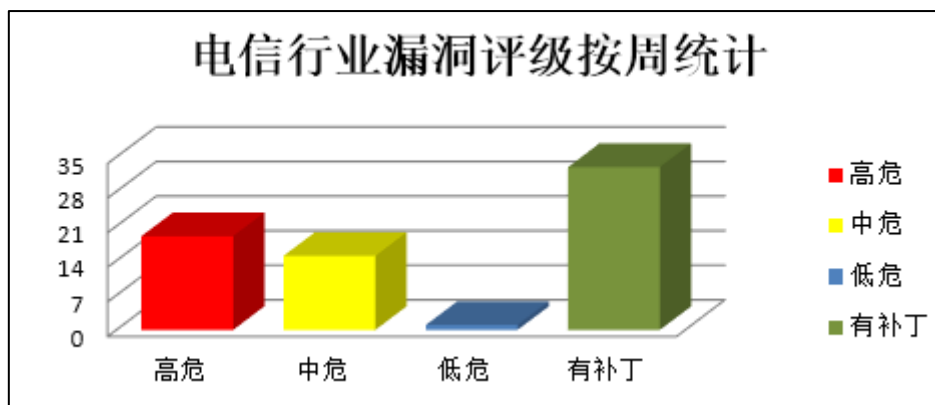


图 1 电信行业漏洞统计

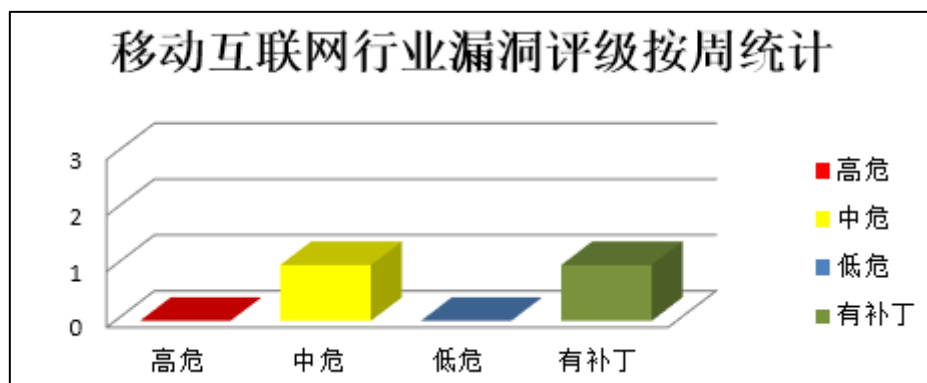


图 2 移动互联网行业漏洞统计

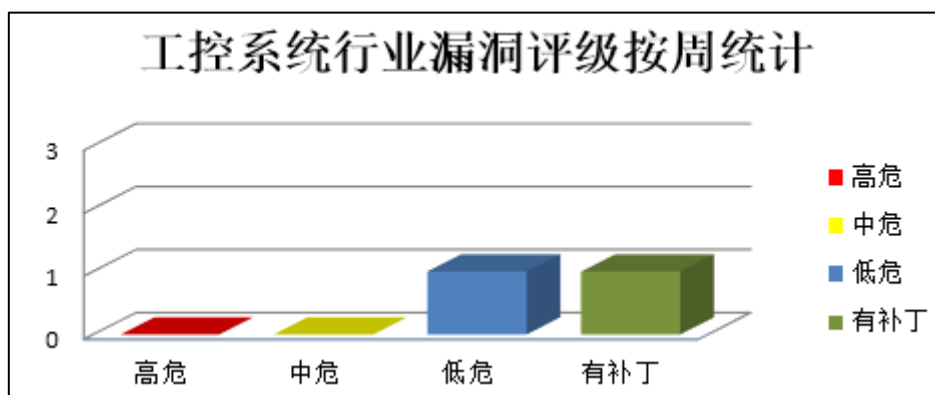


图 3 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Tivoli Storage Manager FastBack 是一套为 Microsoft Windows 和 Linux 服务器提供持续数据保护和恢复管理功能的软件。本周，该产品被披露存在栈缓冲区溢出漏洞，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：IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏

洞（CNVD-2015-04188、CNVD-2015-04187、CNVD-2015-04177、CNVD-2015-04175、CNVD-2015-04176、CNVD-2015-04174、CNVD-2015-04169、CNVD-2015-04170）。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-2015-04188>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04187>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04177>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04175>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04176>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04174>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04169>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04170>

2、Cisco 产品安全漏洞

Nexus 是思科的网络交换机系列产品；Cisco Headend System Releases 是数字宽带传输系统；Cisco Unified Communications Domain Manager（UCDM）是一款用于统一通信解决方案中的呼叫处理组件；Cisco 9900 Series IP Phones 是美国思科(Cisco)公司的 9900 系列 IP 电话产品，该产品提供了语音、视频功能；Cisco IM and Presence Service 可提供企业级即时通讯及网络显现服务；Cisco NX-OS 是一套运行于 Nexus 9000 系列设备中的操作系统。本周，上述产品被披露存在权限提升、拒绝服务、信息泄露和 SQL 注入漏洞。攻击者可利用上述漏洞获取敏感信息、提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Nexus 设备 NS-OS 软件命令行解释器本地权限提升漏洞、Cisco Nexus 设备 Python 子系统本地权限提升漏洞、Cisco Headend System Releases 拒绝服务漏洞、Cisco Unified Communications Domain Manager 信息泄露漏洞、Cisco 9900 Series IP Phones 拒绝服务漏洞、Cisco IM and Presence Service SQL 注入漏洞、Cisco IM and Presence Service 权限提升漏洞、Cisco Nexus 9000 NX-OS 信息泄露漏洞。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-2015-04196>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04202>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04203>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04210>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04201>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04072>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04071>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04073>

3、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，该产品被披露存在安全绕过漏洞。攻击者可利用漏洞绕过安全限制，执行未授权操作。

CNVD 收录的相关漏洞包括：Google Chrome 限制绕过漏洞、Google Chrome Blink 安全绕过漏洞（CNVD-2015-04149、CNVD-2015-04099）、Google Chrome 安全绕过漏洞（CNVD-2015-04100）。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-2015-04192>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04149>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04099>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04100>

4、EMC 产品安全漏洞

EMC Documentum D2 是 Documentum 客户端，可加快 ECM 应用程序的采用速度；EMC Unisphere for VMAX 是高级图形用户接口。本周，上述产品被披露存在 SQL 注入和远程代码执行漏洞。攻击者可利用漏洞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：EMC Documentum D2 SQL 注入漏洞（CNVD-2015-04194、CNVD-2015-04195）、EMC Unisphere for VMAX 远程代码执行漏洞。其中“EMC Unisphere for VMAX 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-2015-04194>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04195>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04079>

5、SQL Buddy 'page'参数目录遍历漏洞

SQL Buddy 是一个 ajax 数据库管理工具。本周，SQL Buddy 被披露存在综合评级为“高危”的目录遍历漏洞。攻击者利用该漏洞可覆盖任意文件。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-2015-04146>

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-2015-04052	1 Click Audio Converter Active X Control 'SkinCrafter.dll' Active X 缓冲区溢出漏洞	高	暂无

CNVD-2015-04063	Decision E-Detective 任意代码执行漏洞	高	暂无
CNVD-2015-04069	SAP Mobile Platform 外部实体漏洞	高	暂无
CNVD-2015-04067	HospiraLifecare PCA Infusion Pump 安全绕过漏洞	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： http://www.hospira.com/en/products_and_services/infusion_pumps/index
CNVD-2015-04076	ZvingSoft SQL 注入漏洞	高	暂无
CNVD-2015-04088	libwmf 堆缓冲区溢出漏洞	高	暂无
CNVD-2015-04087	OSSEC 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://www.ossec.net/?p=1198
CNVD-2015-04086	Project Atomic 安全绕过代码执行漏洞	高	暂无
CNVD-2015-04123	Squashfs 和 sasquatch 'read_fragment_table_4'栈缓冲区溢出漏洞	高	暂无
CNVD-2015-04124	Web Console 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://www.web-console.org/

表 3 部分高危漏洞列表

小结：本周，IBM 产品被披露存在栈缓冲区溢出漏洞漏洞，攻击者可利用漏洞发起拒绝服务攻击。此外，Cisco、Google、EMC 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、绕过安全限制、提升权限、执行任意代码或发起拒绝服务攻击。另外，SQL Buddy 被披露存在一个高危零日漏洞，攻击者利用该漏洞可覆盖任意文件。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、SAP 修补多款产品漏洞

SAP Mobile Platform (SMP) 是德国思爱普 (SAP) 公司的一套移动应用开发平台；SAP NetWeaver 是一套面向服务的集成化应用平台，该平台可为 SAP 应用提供开发和运行环境。

本周，SAP 修补了上述产品存在的信息泄露和权限获取漏洞，避免攻击者利用漏洞

获得敏感信息或访问权限。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/60286>

<http://www.cnvd.org.cn/patchInfo/show/60065>



本周要闻速递

1. 雅虎修复了 SSRF 漏洞

雅虎修复了图片处理系统上的 SSRF（服务端请求伪造）漏洞。SSRF（服务端请求伪造）漏洞，也称 XSPA（跨站端口攻击），漏洞存在于应用程序在加载用户提供的 URL 时，没能正确验证服务器的响应，然后就反馈回了客户端。攻击者可以利用该漏洞绕过访问限制（如防火墙），进而将受感染的服务器作为代理进行端口扫描，甚至是访问系统中的数据。

参考链接：<http://www.freebuf.com/news/71399.html>

2. Android 调试器存在漏洞，可获取设备内存数据

趋势科技近日发现了 Android 调试器 Debuggerd 中的漏洞，一个构造精巧的 ELF(Executable and Linkable Format)文件可以导致调试器崩溃，然后通过 tombstone 文件和对应的 logd 日志文件暴露内存内容。这可以被用于拒绝服务攻击，绕过 ASLR 执行恶意代码。仅仅利用这个漏洞是无法进行代码执行的，但通过这个漏洞暴露的信息可以和其他漏洞结合用于代码执行。漏洞影响的系统版本包括 Android 4.0（Ice Cream Sandwich）到 Lollipop（5.x），下一代的 Android M 已经修复了这个漏洞。

参考链接：<http://www.freebuf.com/news/71157.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