

信息安全漏洞周报

2014 年 12 月 22 日-2014 年 12 月 28 日

2014 年第 52 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 120 个，其中高危漏洞 33 个、中危漏洞 70 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 111 个。本周收录的漏洞中，已有 91 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。本周互联网上出现“ProjectSend r-651 文件上传漏洞”、“JasPer 远程代码执行漏洞”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 家成员单位及个人报送了本周收录的全部 120 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、恒安嘉新、启明星辰、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、深圳市深信服电子科技有限公司、上海天泰网络科技有限公司及白帽子向 CNVD 提交了 1353 个原创漏洞(注：奇虎 360 提交漏洞包含其“库带计划”中部分存量漏洞)。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	1308	1308
天融信	132	0
恒安嘉新	65	0
启明星辰	63	0
安天实验室	58	0

绿盟科技	44	0
CNCERT 贵州分中心	10	10
CNCERT 福建分中心	8	8
CNCERT 江西分中心	5	5
CNCERT 山西分中心	5	5
深圳市深信服电子科技有限公司	7	7
上海天泰网络技术有限公司	2	2
个人	8	8
报送总计	1715	1353
录入总计	120（去重）	1353

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、Honeywell 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	25	21%
2	Cisco	9	8%
3	Honeywell	5	4%
4	ULTRAPOP	4	3%
5	D-Link	3	2%
6	Libvirt	3	2%
7	Drupal	3	2%
8	Apache	2	2%
9	Linux	1	1%
10	其他	65	55%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 120 个漏洞。其中应用程序漏洞 93 个，WEB 应用漏洞 12 个，网络设备漏洞 8 个，安全产品漏洞 3 个，数据库漏洞 3 个，操作系统漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	93
WEB 应用漏洞	12
网络设备漏洞	8
安全产品漏洞	3
数据库漏洞	3
操作系统漏洞	1

表 3 漏洞按影响类型统计表

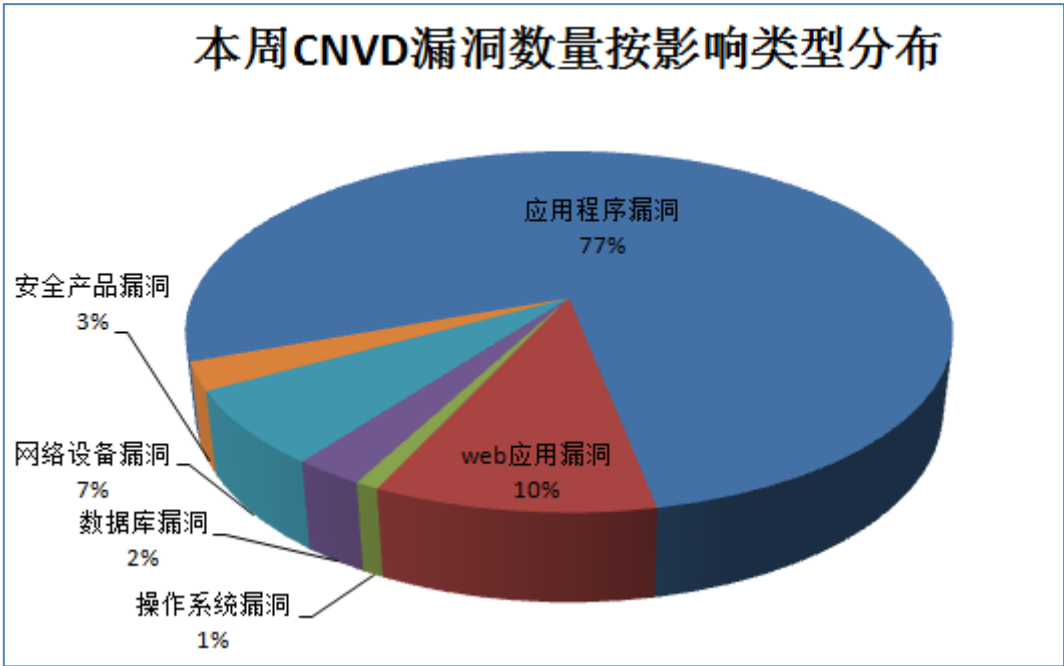


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 25 个电信行业漏洞， 1 个移动互联网行业漏洞，5 个工控系统行业漏洞（如下图表所示）。其中，“多个 Allied Telesis 产品缓冲区溢出漏洞、Allegro RomPager 缓冲区溢出漏洞、Honeywell Experion PKS 存在多个远程堆缓冲区溢出漏洞、Honeywell Experion PKS 存在多个栈缓冲区溢出漏洞、Honeywell Experion PKS ' dual_onsrv.exe'模块远程代码执行漏洞”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-2014-09058	多个 Allied Telesis 产品缓冲区溢出漏洞	高	是
电信	CNVD-2014-09086	Asterisk Open Source 拒绝服务漏洞（C	中	否

		NVD-2014-09086)		
电信	CNVD-2014-09089	IBM WebSphere Portal 跨站脚本漏洞	低	是
电信	CNVD-2014-09088	IBM WebSphere DataPower XC10 appliance 跨站脚本漏洞	低	是
电信	CNVD-2014-09087	IBM WebSphere DataPower XC10 appliance 信息泄露漏洞	低	是
电信	CNVD-2014-09117	Allegro RomPager HTTP Cookie 处理安全绕过漏洞	中	是
电信	CNVD-2014-09123	Allegro RomPager 缓冲区溢出漏洞	高	是
电信	CNVD-2014-09147	Cisco Identity Services Engine Software 特权提升漏洞	中	否
电信	CNVD-2014-09146	Cisco Identity Services Engine 密码泄露漏洞	中	是
电信	CNVD-2014-09136	D-Link DIR-655 跨站脚本漏洞	中	是
电信	CNVD-2014-09135	D-Link DIR-655 安全绕过漏洞	中	是
电信	CNVD-2014-09134	D-Link DIR-655 信息泄露漏洞	中	是
电信	CNVD-2014-09166	IBM WebSphere Service Registry and Repository (WSRR)会话劫持漏洞	低	是
电信	CNVD-2014-09154	ARRIS Touchstone TG862G/CT Telephony Gateway 安全机制绕过漏洞	高	否
电信	CNVD-2014-09177	Mobilis 3g MobiConnect 3G++ ZDServ er 权限提升漏洞	中	否
电信	CNVD-2014-09172	IBM WebSphere Service Registry and Repository (WSRR)跨站脚本漏洞 (CNVD-2014-09172)	低	是
电信	CNVD-2014-09171	IBM WebSphere Service Registry and Repository (WSRR)跨站请求伪造漏洞	低	是
电信	CNVD-2014-09170	IBM WebSphere Service Registry and Repository (WSRR)访问限制漏洞	低	是
电信	CNVD-2014-09169	IBM WebSphere Service Registry and Repository (WSRR)信息泄露漏洞 (CNVD-2014-09169)	低	是
电信	CNVD-2014-09173	IBM WebSphere Service Registry and Repository (WSRR)跨站脚本漏洞 (CNVD-2014-09173)	低	是
电信	CNVD-2014-09174	IBM WebSphere Service Registry and Repository (WSRR)跨站脚本漏洞 (CNVD-2014-09174)	中	是
电信	CNVD-2014-09175	IBM WebSphere Service Registry and Repository (WSRR)跨站脚本漏洞 (CNVD-2014-09175)	低	是
电信	CNVD-2014-09168	IBM WebSphere Service Registry and Repository (WSRR)信息泄露漏洞 (CNVD-2014-09168)	中	是

电信	CNVD-2014-09167	IBM WebSphere Service Registry and Repository (WSRR)目录遍历漏洞	中	是
电信	CNVD-2014-09176	IBM WebSphere Service Registry and Repository (WSRR)跨站脚本漏洞 (CNVD-2014-09176)	低	是
移动互联网	CNVD-2014-09155	AppsGeyser for Android SSL 证书校验安全绕过漏洞	中	否
工控系统	CNVD-2014-09113	Honeywell Experion PKS 存在多个远程堆缓冲区溢出漏洞	高	是
工控系统	CNVD-2014-09112	Honeywell Experion PKS 'confd.exe'模块目录遍历漏洞	中	是
工控系统	CNVD-2014-09111	Honeywell Experion PKS 文件包含漏洞	中	是
工控系统	CNVD-2014-09120	Honeywell Experion PKS 存在多个栈缓冲区溢出漏洞	高	是
工控系统	CNVD-2014-09114	Honeywell Experion PKS 'dual_onsrv.exe'模块远程代码执行漏洞	高	是

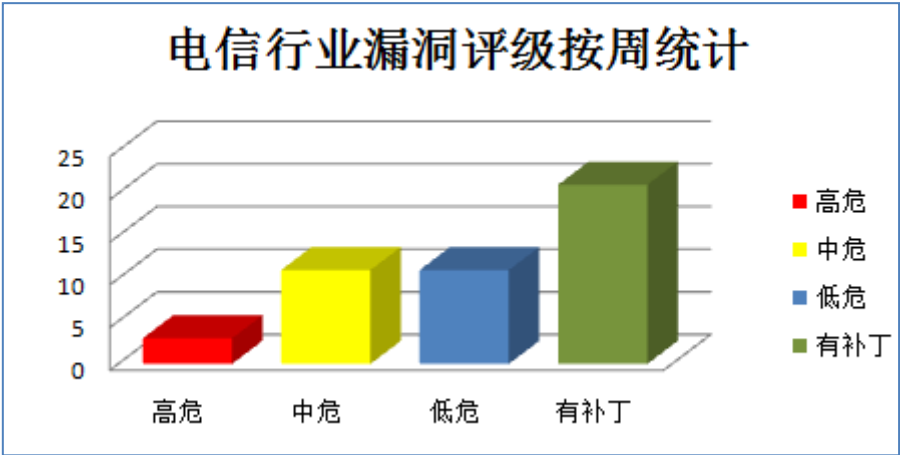


图 1 电信行业漏洞统计

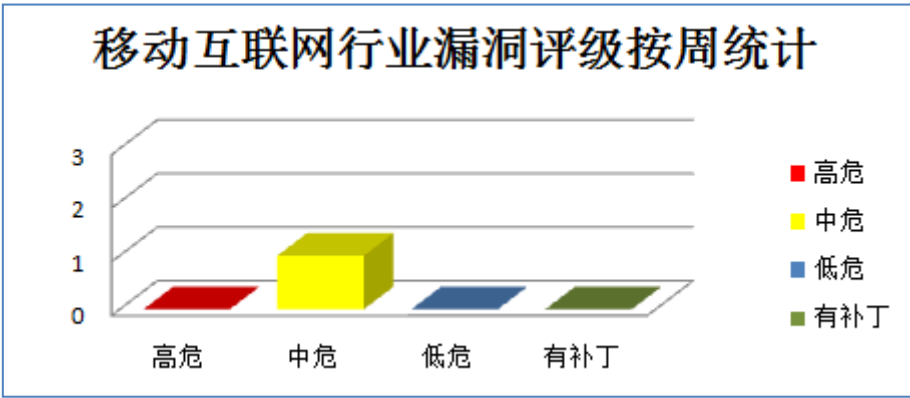


图 2 移动互联网行业漏洞统计

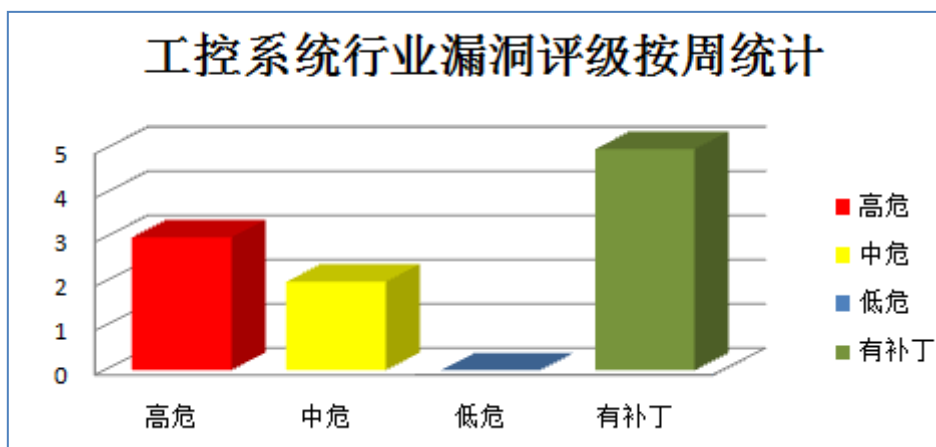


图 3 工控系统行业漏洞统计

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 WebSphere Service Registry and Repository (WSRR) 是美国 IBM 公司的一个用于服务交互端点描述的主元数据存储库，它提供了存储、访问和管理有关服务信息的功能，并且是 SOA 实现的关键组成部分。本周，上述产品被披露存在跨站脚本、信息泄露和目录遍历漏洞，攻击者可利用漏洞进行跨站攻击或获取敏感信息。

CNVD 收录的相关漏洞包括：IBM WebSphere Service Registry and Repository (WSRR) 跨站脚本漏洞 (CNVD-2014-09176、CNVD-2014-09175、CNVD-2014-09174、CNVD-2014-09173、CNVD-2014-09172)、IBM WebSphere Service Registry and Repository (WSRR) 信息泄露漏洞 (CNVD-2014-09168、CNVD-2014-09169)、IBM WebSphere Service Registry and Repository (WSRR) 目录遍历漏洞。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-2014-09176>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09175>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09174>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09173>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09172>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09168>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09169>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09167>

2、Cisco 产品安全漏洞

Cisco Unified Communications 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Jabber Guest 支持即将实施的 WebRTC 标准，可与 Cisco Contact Center Enterprise 解决方案组合使用。Cisco Identity Services Engine 身份服务引擎是一款用于 Cisco TrustSec 解决方案的中央策略引擎。Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞提升权限、获取敏感信息或进行跨站攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Domain Manager 跨站脚本漏洞（CNVD-2014-09142）、Cisco Jabber Guest 存在多个信息泄露漏洞（CNVD-2014-09143）、Cisco Jabber Guest Server 存在多个跨站脚本漏洞、Cisco Jabber Guest 存在多个信息泄露漏洞、Cisco Identity Services Engine 密码泄露漏洞、Cisco Identity Services Engine Software 特权提升漏洞、Cisco Adaptive Security Appliance (ASA) 信息泄露漏洞、Cisco Enterprise Content Delivery System (ECDS) 任意文件访问漏洞。其中，“Cisco Identity Services Engine 密码泄露漏洞”厂商已经发布了该漏洞的修补程序。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-2014-09142>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09143>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09144>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09145>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09146>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09147>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09148>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09140>

3、D-Link 产品安全漏洞

DIR-655 全球首款通过 Windows Vista 认证的无线路由器无线开关定时器。本周，上述产品被披露存在信息泄露、安全绕过、跨站脚本漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括：D-Link DIR-655 信息泄露漏洞、D-Link DIR-655 安全绕过漏洞、D-Link DIR-655 跨站脚本漏洞。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-2014-09134>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09135>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09136>

4、NetIQ 产品安全漏洞

NetIQ Access Manager 是一款访问控制管理程序。NetIQ eDirectory 是一个 LDAP 目录服务。本周，上述产品被披露存在信息泄露、跨站脚本和跨站请求伪造漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括：NetIQ Access Manager 跨站请求伪造漏洞、NetIQ Access Manager 存在多个信息泄露漏洞、NetIQ eDirectory NDS iMonitor 远程信息泄露漏洞、NetIQ Access Manager 存在多个漏洞、NetIQ eDirectory NDS iMonitor 跨站脚本漏洞。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-2014-09109>
<http://www.cnvd.org.cn/ flaw/show/CNVD-2014-09110>
<http://www.cnvd.org.cn/ flaw/show/CNVD-2014-09115>
<http://www.cnvd.org.cn/ flaw/show/CNVD-2014-09116>
<http://www.cnvd.org.cn/ flaw/show/CNVD-2014-09119>

5、SAP BusinessObjects Edge 权限提升漏洞

SAP BusinessObjects 是一款商务智能软件和企业绩效解决方案。本周，SAP BusinessObjects 被披露存在综合评级为“高危”的权限提升漏洞。攻击者可以利用此漏洞提升权限。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-2014-09152>

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-2014-09053	ULTRAPOP.JP i-HTTPD 任意命令执行漏洞	高	暂无
CNVD-2014-09048	PHP 'ext/standard/var_unserializer.re'内存错误引用漏洞	高	用户可以联系供应商获得补丁信息： http://php.net/ChangeLog-5.php
CNVD-2014-09052	Innominate mGuard 未授权修改漏洞	高	用户可以联系供应商获得补丁信息： http://www.innominate.com/en/
CNVD-2014-09057	Hopper Mach-O Loader 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： http://hopperapp.com/
CNVD-2014-09065	Git 任意代码执行漏洞	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： https://www.kernel.org/pub/software/scm/git/

			https://kernel.googlesource.com/pub/scm/git/git https://code.google.com/p/git-core/ https://github.com/gitster/git
CNVD-2014-09064	GLPI 盲 SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.glpi-project.org/spip.php?page=annonce&id_breve=334&lang=en
CNVD-2014-09063	miniBB 'code' SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.minibb.com/forums/news-9/blind-sql-injection-fix-6430.html http://security.szurek.pl/minibb-31-blind-sql-injection.html
CNVD-2014-09096	SafeNet Authentication Service Outlook Web Access Agent 目录遍历漏洞	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://appcheck-ng.com/safenet-sas-owa-agent-directory-traversal-vulnerability/
CNVD-2014-09092	EMC Documentum Content Server 权限提升漏洞	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.emc.com/domains/documentum/index.htm
CNVD-2014-09094	Movable Type SQL 注入漏洞	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://secunia.com/advisories/61227

表 3 部分高危漏洞列表

小结：本周，IBM 产品被批露存在跨站脚本和目录遍历漏洞，攻击者可利用漏洞进行跨站攻击或获取敏感信息。Cisco、D-Link、NetIQ 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞提升权限、获取敏感信息、进行跨站攻击或执行未授权操作。此外，SAP BusinessObjects Edge 被批露存在一个高危零日漏洞。攻击者可以利用此漏洞提升权限。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、Linux 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的拒绝服务漏洞，避免攻击者通过特制的应用程序获得特权或发起拒绝服务攻击。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/53236>

本周要闻速递

1. 恶意软件 Soaksoak 卷土重来

前不久，Soaksoak 曾因感染了十万多个 wordpress 网站而名声大噪，从上周日的情况来看，Soaksoak 大有卷土重来之势。Soaksoak 恶意软件，来源于 SoakSoak.ru，其主要攻击手段是通过 RevSlider 的漏洞作为切入点，上传一个后门，然后对所有使用相同服务器的网站进行感染。这就意味着即使该网站不使用 RevSlider 也会被感染，被感染的 visitor-facing 部分主要包含 wp-includes/js/swfobject.js 及 wp-includes/template-loader.php 两个文件。对被感染的网站进行更为详尽的检测后发现，该恶意软件出现了变种，除了上面两种文件，还有一个名为 wp-includes/js/swfobject.swf 的文件（不包含后门和 RevSlider 的漏洞）也同样会导致感染。

参考链接：<http://www.freebuf.com/news/54883.html>

2. SS7 协议曝漏洞

最近，有德国的研究人员发现 SS7 协议存在巨大安全漏洞，该漏洞可导致用户的电话和短信数据遭到大规模的窃听和盗取，而且更可怕的是，即使使用了最新的蜂窝网络和最先进的加密技术也无济于事。该漏洞来自全球知名的电信网络协议 Signal System 7 (SS7)，目前世界上有许多电信运营商都在使用 SS7（包括 AT&T 和 Verizon），为用户提供电话，短信以及其他服务。由于其许多基础结构都已经过时，所以很容易遭到黑客攻击。德国的研究人员将本月早些时候在汉堡举行的黑客会议上公布他们发现的漏洞详情。

参考链接：<http://www.freebuf.com/news/54754.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