

信息安全漏洞周报

2015 年 04 月 27 日-2015 年 05 月 03 日

2015 年第 18 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 102 个，其中高危漏洞 32 个、中危漏洞 59 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 89 个。本周收录的漏洞中，已有 87 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 插件 TheCartPress 本地 PHP 文件包含漏洞”、“ProFTPD (mod_copy)远程命令执行漏洞”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 5 家成员单位、合作伙伴及个人报送了本周收录的全部 102 个漏洞。报送情况如表 1 所示。其中，启明星辰、恒安嘉新、天融信、绿盟科技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、安徽讯成创安科技有限公司、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 190 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	83	0
恒安嘉新	53	0
天融信	49	4
绿盟科技	41	0
安天实验室	30	0

乌云	158	158
漏洞盒子	18	18
High-Tech Bridge Security Research Lab	3	3
深圳市深信服电子科 技有限公司	1	1
安徽讯成创安科技有 限公司	1	1
CNCERT 山西分中心	1	1
个人	4	4
报送总计	442	190
录入总计	102（去重）	190

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、WordPress、Cisco 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	13	13%
2	WordPress	8	8%
3	Cisco	7	7%
4	Novell	7	7%
5	Linux	6	6%
6	HP	4	4%
7	Haxx	4	4%
8	SQLite	3	3%
9	Apple	2	2%
10	其他	48	46%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 102 个漏洞。其中应用程序漏洞 68 个，WEB 应用漏洞 14 个，操作系统漏洞 8 个，网络设备漏洞 8 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	68
WEB 应用漏洞	14
操作系统漏洞	8
网络设备漏洞	8
数据库漏洞	4

表 3 漏洞按影响类型统计表

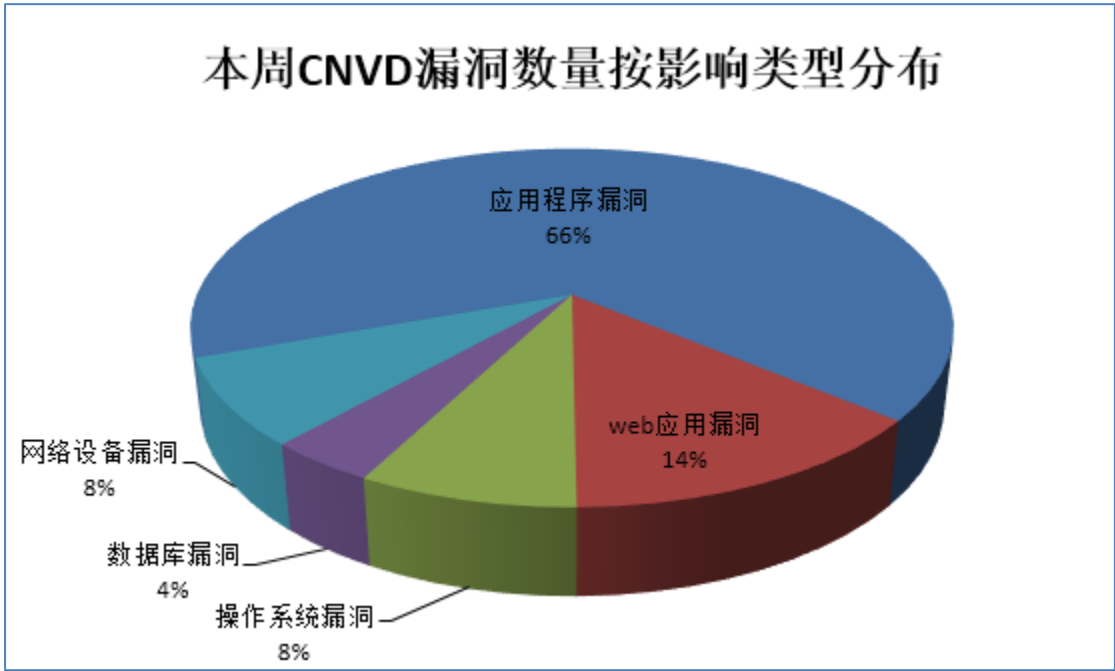


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 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，“Samsung Galaxy S5 指纹数据泄露漏洞、IBM WebSphere Application Server (WAS)权限提升漏洞（CNVD-2015-02799、CNVD-2015-02800）”的综合评级均为“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-2015-02757	IBM WebSphere MQ XR WebSockets Listener 跨站脚本漏洞	中	是
电信	CNVD-2015-02768	ZYXEL P-660HN-T1H_IPv6 远程配置编辑器/Web 服务器拒绝服务漏洞	中	否
电信	CNVD-2015-02787	Samsung Galaxy S5 指纹数据泄露漏洞	高	是

电信	CNVD-2015-02799	IBM WebSphere Application Server (WAS)权限提升漏洞 (CNVD-2015-02799)	高	是
电信	CNVD-2015-02800	IBM WebSphere Application Server (WAS)权限提升漏洞 (CNVD-2015-02800)	高	是
电信	CNVD-2015-02806	IBM WebSphere Application Server (WAS)权限提升漏洞 (CNVD-2015-02806)	中	是
电信	CNVD-2015-02801	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2015-02801)	中	是
电信	CNVD-2015-02802	IBM WebSphere Portal 拒绝服务漏洞	中	是
电信	CNVD-2015-02809	IBM WebSphere Application Server (WAS) SNMP 实现敏感信息泄露漏洞	低	是
电信	CNVD-2015-02813	Cisco IOS 和 IOS-XE 拒绝服务漏洞 (CNVD-2015-02813)	中	是
电信	CNVD-2015-02812	Cisco IOS 和 IOS-XE 拒绝服务漏洞 (CNVD-2015-02812)	中	是
电信	CNVD-2015-02814	Cisco IOS XE Overlay Transport Virtualization 拒绝服务漏洞	中	是
移动互联网	CNVD-2015-02787	Samsung Galaxy S5 指纹数据泄露漏洞	高	是
工控系统	CNVD-2015-02759	HP Network Automation 存在多个漏洞	中	是

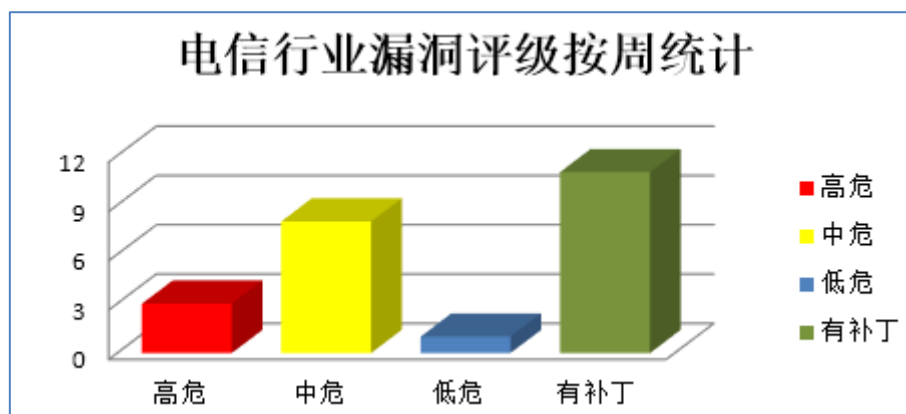


图 1 电信行业漏洞统计

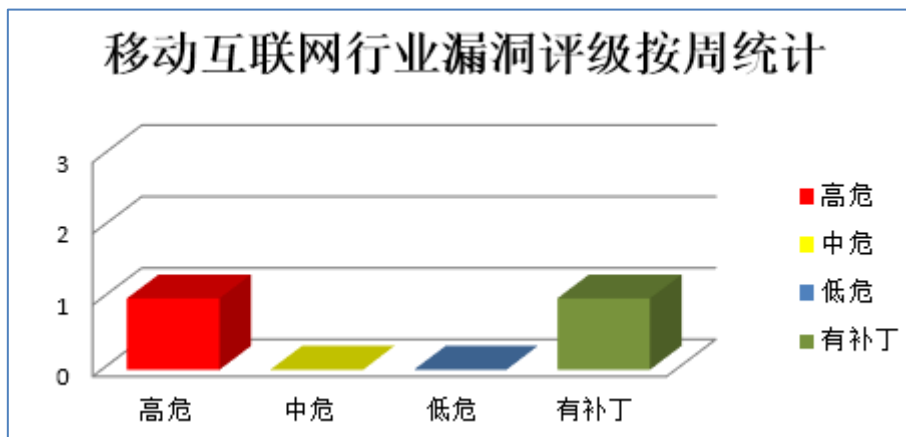


图 2 移动互联网系统行业漏洞统计

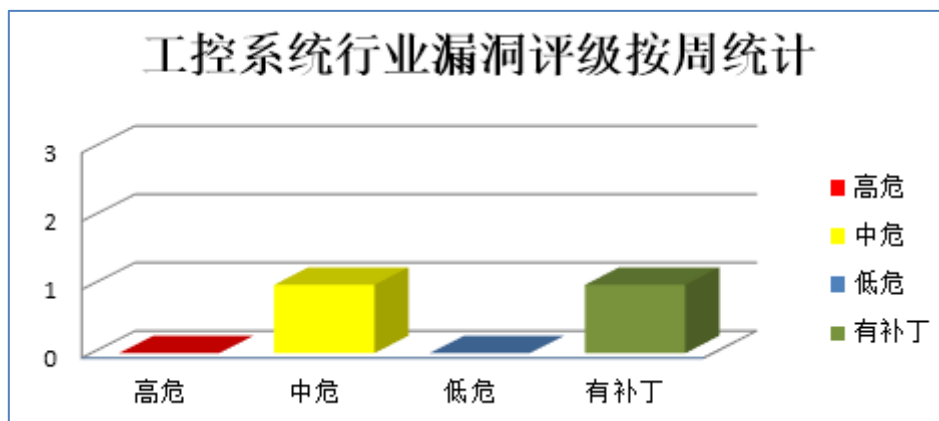


图 3 工控系统行业漏洞统计

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 Portal 由用于构建和管理安全的企业对企业（B2B）、企业对客户（B2C）和企业对雇员（B2E）门户网站的中间件、应用程序（称为 portlet）和开发工具组成。IBM WebSphere Application Server（WAS）是美国 IBM 公司开发并发行的一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM Sterling Order Management 是一套订单管理软件，能够协调跨客户、供应商和合作伙伴动态业务网络的跨渠道销售和订单实现过程。IBM Curam Social Program Management（SPM）是美国 IBM 公司的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。本周，上述产品被披露存在权限提升、拒绝服务、跨站脚本和跨站请求伪造漏洞。攻击者可利用漏洞提升权限、进行跨站脚本和跨站请求伪造攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server (WAS)权限提升漏洞（CNVD-2015-02800、CNVD-2015-02799、CNVD-2015-02806）、IBM WebSphere Portal 跨站脚本漏洞（CNVD-2015-02801）、IBM WebSphere Portal 拒绝服务漏洞、IBM Curam Social Program Management 拒绝服务漏洞、IBM Curam Social Program Management (SPM)跨站请求伪造漏洞（CNVD-2015-02805）、IBM Sterling Order Management 跨站脚本漏洞（CNVD-2015-02756）。其中“IBM WebSphere Application Server (WAS)权限提升漏洞（CNVD-2015-02800、CNVD-2015-02799）”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-2015-02800>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02799>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02806>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02801>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02802>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02803>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02805>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02756>

2、Cisco 产品安全漏洞

Cisco IOS 和 IOS-XE 都是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco ASR 5000 Series 是美国思科（Cisco）公司的 5000 系列无线控制器产品。StarOS 是一套运行于 5000 系列无线控制器产品中为移动服务和网络动态分配资源的虚拟化操作系统。Cisco FireSIGHT Management Center 是美国思科（Cisco）公司的一套支持集中管理采用 FirePOWER Services 的 Cisco ASA 和思科 FirePOWER 网络安全设备的网络安全和运行功能的管理中心软件。Cisco Secure Access Control Server Solution Engine 是一个思科安全访问控制服务器解决方案引擎。本周，上述产品被披露存在拒绝服务、开放重定向、跨站脚本和跨站请求伪造漏洞。攻击者可利用漏洞进行跨站脚本和跨站请求伪造攻击、重定向页面或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS 和 IOS-XE 拒绝服务漏洞（CNVD-2015-02812、CNVD-2015-02813）、Cisco IOS XE Overlay Transport Virtualization 拒绝服务漏洞、Cisco ASR 5000 Series StarOS 拒绝服务漏洞、Cisco FireSIGHT Management Center FireSIGHT System Software 开放重定向漏洞、Cisco FireSIGHT Management Center FireSIGHT System Software 跨站脚本漏洞、Cisco Secure Access Control Server Dashboard 页面跨站请求伪造漏洞。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-2015-02812>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02813>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02814>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02815>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02721>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02726>

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，上述产品被披露存在权限提升、拒绝服务、缓冲区溢出和安全绕过漏洞。攻击者可利用漏洞提升权限、绕过沙箱限制或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 'btrfs/ctree.c'本地权限提升漏洞、Linux kernel TCP Fast Open 拒绝服务漏洞、Linux kernel AESNI 缓冲区溢出漏洞、Linux kernel Netfilter Connection Tracking Extension 加载拒绝服务漏洞、Linux kernel int80 32-Bit Emulation 安全绕过漏洞、Linux kernel chown()权限提升漏洞。其中“Linux kernel 'btrfs/ctree.c'本地权限提升漏洞、Linux kernel AESNI 缓冲区溢出漏洞、Linux kernel chown()权限提升漏洞”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-2015-02796>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02761>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02762>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02763>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02764>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02724>

4、Novell 产品安全漏洞

Novell ZENworks 是一套支持在组织内跨资源进行自动化 IT 管理和业务流程管理的软件。本周，上述产品被披露存在信息泄露、缓冲区溢出、SQL 注入和远程代码执行漏洞。攻击者可利用漏洞获取敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：Novell ZENworks 会话 ID 泄露漏洞、Novell ZENworks 'ScheduleQuery'方法 SQL 注入漏洞、Novell ZENworks 'GetReRequestData'方法 SQL 注入漏洞、Novell ZENworks 'doPost'方法远程代码执行漏洞、Novell ZENworks 'FileViewer'类信息泄露漏洞、Novell ZENworks Preboot Policy Service 缓冲区溢出漏洞、Novell ZENworks 'dirname'信息泄露漏洞。其中“Novell ZENworks Preboot Policy Service 缓冲区溢出漏洞”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-2015-02830>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02831>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02832>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02833>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02829>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02742>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02741>

5、Realtek rtl81xx miniigd SOAP 服务远程代码执行漏洞

Realtek rtl81xx SDK 是瑞昱（Realtek）公司的一套 rtl81xx 系列网卡驱动及 SDK 开发包。本周，Realtek rtl81xx SDK 被披露存在综合评级为“高危”的远程代码执行漏洞。攻击者利用该漏洞可以‘root’权限执行任意代码。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-2015-02823>

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-2015-02725	Mozilla Firefox 'AsyncPaintWaitEvent::AsyncPaintWaitEvent()' 内存错误引用漏洞	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: https://www.mozilla.org/en-US/security/advisories/mfsa2015-45/
CNVD-2015-02731	New Atlanta BlueDragon 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://seclists.org/fulldisclosure/2015/Apr/49
CNVD-2015-02737	wpa_supplicant P2P SSID 处理漏洞	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://w1.fi/security/2015-1/
CNVD-2015-02754	cURL 和 libcurl 拒绝服务漏洞 (CNVD-2015-02754)	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://curl.haxx.se/docs/adv_20150422B.html
CNVD-2015-02753	cURL 和 libcurl 拒绝服务漏洞 (CNVD-2015-02753)	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://curl.haxx.se/docs/adv_20150422B.html
CNVD-2015-02750	SQLite 拒绝服务漏洞 (CNVD-2015-02750)	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://www.sqlite.org/releaselog/3_8_9.html
CNVD-2015-02749	SQLite 拒绝服务漏洞 (CNVD-2015-02749)	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://www.sqlite.org/releaselog/3_8_9.html
CNVD-2015-02748	SQLite 拒绝服务漏洞 (CNVD-2015-02748)	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://www.sqlite.org/releaselog/3_8_9.html
CNVD-2015-02772	SevenIT SevDesk 存在多个输入验证漏洞	高	用户可联系供应商获得补丁信息: https://sevdesk.de/

表 3 部分高危漏洞列表

小结: 本周, IBM 多款产品被批露存在权限提升、拒绝服务、跨站脚本和跨站请求伪造漏洞。攻击者可利用漏洞提升权限、进行跨站脚本和跨站请求伪造攻击。此外, Ci

sco、Linux、Novell 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、执行任意代码、进行跨站脚本和跨站请求伪造攻击或发起拒绝服务攻击。另外，Realtek rtl81xx SDK 被披露存在一个高危零日漏洞，攻击者利用该漏洞可以‘root’权限执行任意代码。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、SAP 修补 Adaptive Server Enterprise 产品漏洞

SAP Sybase Adaptive Server Enterprise (ASE) 是德国思爱普 (SAP) 公司的一套关系型数据库管理系统。该系统可在数据密集型环境中使用，并具有速度快、性能稳定等特点。

本周，SAP 修补了上述产品存在的安全绕过漏洞，避免攻击者利用漏洞绕过安全限制。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/57922>

本周要闻速递

1. MySQL SSL/TLS 连接存在安全漏洞，可遭中间人攻击

由于客户端在连接 MySQL 时 SSL 选项使用不当，将可能引起中间人攻击。该漏洞与客户端的“-ssl”选项有着很大关系，这个选项在受影响的版本中处于“建议使用”的级别。因此，当客户端尝试和服务端进行初始化 SSL/TLS 连接时，将不会要求使用这一选项。这就帮助 MITM 攻击者轻易地去除了 SSL/TLS 保护。这个问题同样影响到了 SSL 客户端的其它 SSL 选项上（比如“-ssl-xxx”）。Oracle MySQL 的技术产品主管也在 blog 中对“-ssl”问题进行了具体的说明。

参考链接：<http://www.freebuf.com/news/66277.html>

2. 友讯 (D-Link)、趋势网络路由器曝远程代码执行漏洞

由于使用了 Realtek 瑞昱公司存在漏洞的软件开发工具包 (SDK)，友讯科技、趋势网络以及其他品牌路由器很容易被攻击者远程执行任意代码。该漏洞 (CVE-2014-8361) 允许未经身份验证的攻击者使用 root 特权在受害者系统上执行任意代码。

参考链接：<http://www.freebuf.com/news/66195.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