

信息安全漏洞周报

2014 年 7 月 21 日-2014 年 7 月 27 日

2014年第30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**高**。

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 262 个，其中高危漏洞 61 个、中危漏洞 160 个、低危漏洞 41 个。上述漏洞中，可利用来实施远程攻击的漏洞有 228 个。本周收录的漏洞中，已有 213 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“Ato mCMS admin/uploads.php SQL 注入漏洞”、“WEBMIS CMS 任意文件上传漏洞”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 7 家成员单位、合作伙伴及个人报送了本周收录的全部 262 个漏洞。报送情况如表 1 所示。其中，天融信、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、High-Tech BridgeSecurity Research 及白帽子向 CNVD 提交了 84 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	202	0
启明星辰	128	0
安天实验室	110	0
绿盟科技	92	0
恒安嘉新	89	0
奇虎 360	58	58

东软	6	0
High-Tech Bridge Security Research	1	1
CNCERT 福建分中心	4	4
CNCERT 江西分中心	3	3
CNCERT 新疆分中心	3	3
CNCERT 重庆分中心	3	3
CNCERT 山西分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 山东分中心	1	1
个人	7	7
报送总计	711	84
录入总计	262（去重）	84

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Mozilla、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	Oracle	60	30%
2	Mozilla	14	5%
3	WordPress	13	5%
4	Moodle	13	5%
5	IBM	13	5%
6	Apache	7	3%
7	Cisco	7	3%
8	Cybozu	6	2%
9	Drupal	5	2%
10	其他	124	40%

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 262 个漏洞。其中应用程序漏洞 186 个，WEB 应用漏洞 42 个，数据库漏洞 13 个，网络设备漏洞 12 个，操作系统漏洞 6 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	186
WEB 应用漏洞	42
数据库漏洞	13
网络设备漏洞	12
操作系统漏洞	6
安全产品漏洞	3

表 3 漏洞按影响类型统计表

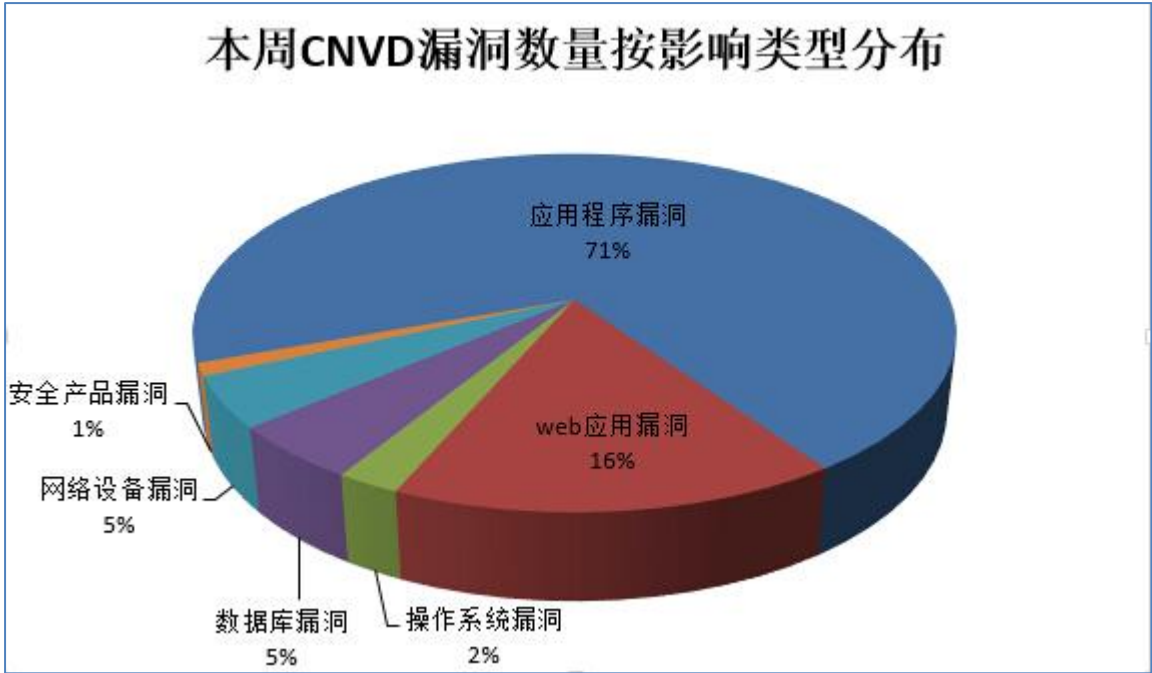


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 33 个电信行业漏洞，3 个移动互联网漏洞，5 个工控系统漏洞（如下图表所示）。其中，“多个 D-Link 产品'soap.cgi'远程命令注入漏洞、Advantech W ebAccess 密码泄露漏洞、Advantech WebAccess 多个 ActiveX 控件缓冲区溢出漏洞、Ad vantech WebAccess 远程验证绕过漏洞、Advantech WebAccessbwocxrun 不安全 ActiveX 控件信息泄露漏洞”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-2014-04252	Cisco Unified Communications Manage r 目录遍历漏洞（CNVD-2014-04252）	中	否
电信	CNVD-2014-04414	Oracle MySQL SRFTS 子件存在未明漏洞	中	是

电信	CNVD-2014-04415	Oracle MySQL ENARC 子件存在未明漏洞	中	是
电信	CNVD-2014-04416	Oracle MySQL SROPTZR 子件存在未明漏洞	中	是
电信	CNVD-2014-04418	Oracle MySQL SRSP 子件存在未明漏洞	低	是
电信	CNVD-2014-04419	Oracle MySQL SRREP 子件存在未明漏洞（CNVD-2014-04419）	中	是
电信	CNVD-2014-04417	Oracle MySQL SROPTZR 子件存在未明漏洞（CNVD-2014-04417）	中	是
电信	CNVD-2014-04420	Oracle MySQL SRREP 子件存在未明漏洞（CNVD-2014-04420）	低	是
电信	CNVD-2014-04411	Oracle WebLogic Server 存在未明漏洞	中	是
电信	CNVD-2014-04412	Oracle WebLogic Server 存在未明漏洞（CNVD-2014-04412）	中	是
电信	CNVD-2014-04413	Oracle WebLogic Server WLS Core 子件存在未明漏洞	中	是
电信	CNVD-2014-04421	Oracle MySQL ENFED 子件存在未明漏洞	低	是
电信	CNVD-2014-04422	Oracle MySQL SRINFOSC 子件存在未明漏洞	中	是
电信	CNVD-2014-04423	Oracle MySQL SRCHAR 子件存在未明漏洞	中	是
电信	CNVD-2014-04424	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04424）	中	是
电信	CNVD-2014-04425	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04425）	中	是
电信	CNVD-2014-04429	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04429）	中	是
电信	CNVD-2014-04426	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04426）	中	是
电信	CNVD-2014-04427	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04427）	中	是
电信	CNVD-2014-04428	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04428）	中	是
电信	CNVD-2014-04430	Oracle WebLogic Server WLS - Web Services 子件存在未明漏洞（CNVD-2014-04430）	中	是

电信	CNVD-2014-04458	Cisco IOS XR Software MPLS 数据包处理拒绝服务漏洞	中	是
电信	CNVD-2014-04468	Oracle WebLogic Server Console 子件存在未明漏洞	中	是
电信	CNVD-2014-04467	Oracle WebLogic Server JVM 子件存在未明漏洞	中	是
电信	CNVD-2014-04466	Oracle WebLogic Server WLS - Security and Policy 子件存在未明漏洞	中	是
电信	CNVD-2014-04465	Oracle WebLogic Server WLS - Deployment 子件存在未明漏洞	中	是
电信	CNVD-2014-04505	多个 D-Link 产品'soap.cgi'远程命令注入漏洞	高	是
电信	CNVD-2014-04502	Oracle Fusion Middleware Process Mgmt& Notification 子件存在未明漏洞	中	是
电信	CNVD-2014-04499	Oracle Database Server RDBMS Core 组件存在未明漏洞 (CNVD-2014-04499)	中	是
电信	CNVD-2014-04500	Oracle Database Server RDBMS Core 组件存在未明漏洞 (CNVD-2014-04500)	中	是
电信	CNVD-2014-04501	Oracle Database Server RDBMS Core 组件存在未明漏洞 (CNVD-2014-04501)	低	是
电信	CNVD-2014-04522	Cisco Unified Communications Manager 拨号分析程序跨站脚本漏洞	中	是
电信	CNVD-2014-04591	Oracle Fusion Middleware 存在未明漏洞	中	是
移动互联网	CNVD-2014-04448	Boat Browser WebView 类远程执行代码漏洞	高	否
移动互联网	CNVD-2014-04503	安卓 Puffin Web Browser 地址栏伪造漏洞	中	否
移动互联网	CNVD-2014-04570	NextApp File Explorer for Android 目录遍历漏洞	中	是
工控系统	CNVD-2014-04462	Advantech WebAccess 远程代码执行漏洞	中	是
工控系统	CNVD-2014-04530	Advantech WebAccess 密码泄露漏洞	高	是
工控系统	CNVD-2014-04544	Advantech WebAccess 多个 ActiveX 控件缓冲区溢出漏洞	高	是
工控系统	CNVD-2014-04531	Advantech WebAccess 远程验证绕过漏洞	高	是
工控系统	CNVD-2014-04532	Advantech WebAccessbwocxrun 不安全 ActiveX 控件信息泄露漏洞	高	是

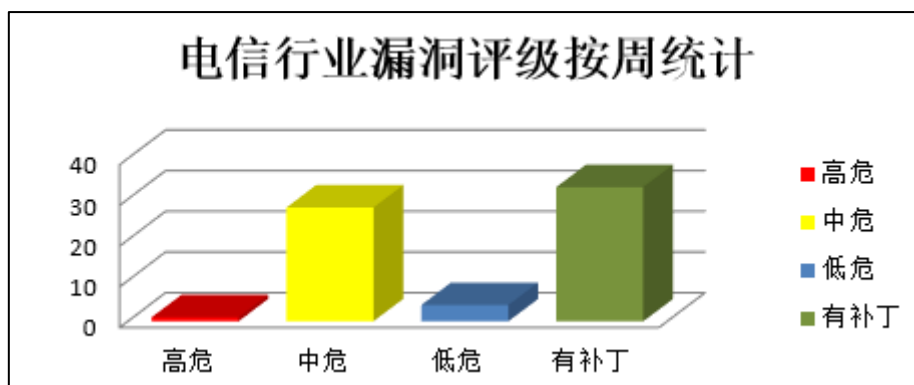


图 1 电信行业漏洞统计

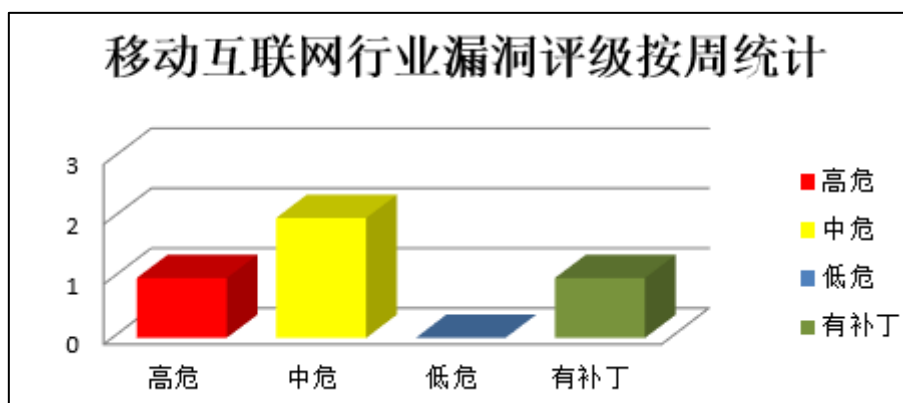


图 2 移动互联网行业漏洞统计

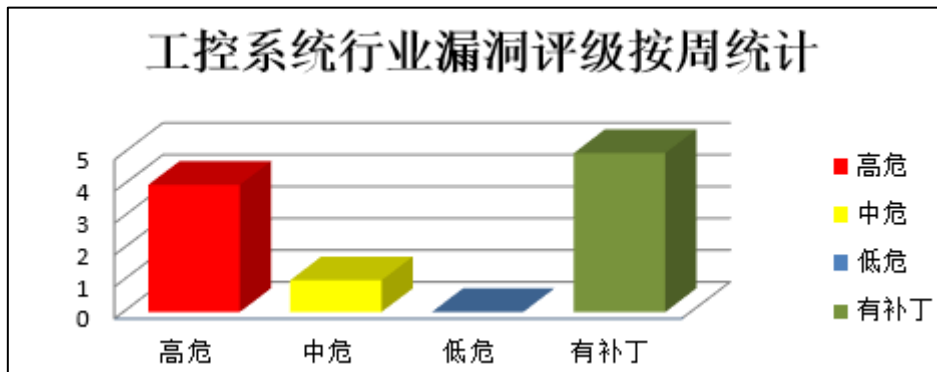


图 3 工控系统行业漏洞统计

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、Mozilla 产品安全漏洞

Firefox/Thunderbird/SeaMonkey 是 Mozilla 所发布的 WEB 浏览器和邮件/新闻组客户端。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞构建恶意 WEB 页，诱使用户解析，可执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird 内存破坏漏洞（CNVD-2014-04595）、Mozilla Firefox/Thunderbird Skia 远程代码执行漏洞、Mozilla Firefox/Thunderbird FireOnStateChange 内存错误引用远程代码执行漏洞、Mozilla Firefox/Thunderbird Cesium JS 远程代码执行漏洞、Mozilla Firefox/Thunderbird WebAudio 内存错误引用远程代码执行漏洞、Mozilla Firefox/Thunderbird DirectWrite 内存错误引用远程代码执行漏洞、Mozilla Firefox/Thunderbird WebAudio 堆缓冲区溢出漏洞、Mozilla Firefox/Thunderbird 存在多个内存破坏漏洞（CNVD-2014-04607）。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-2014-04595>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04601>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04603>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04602>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04606>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04605>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04614>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04607>

2、IBM 产品安全漏洞

IBM InfoSphere Master Data Management Server for Product Information Management（IBM InfoSphere MDM Server for PIM）是美国 IBM 公司的一套企业产品信息管理解决方案。IBM InfoSphere Master Data Management（MDM）- Collaborative Edition 是一套为产品信息管理（PIM）提供协同编辑的解决方案。IBM 1754 GCM 系列在单一设备中提供了经由 IP 的 KVM 和串行控制台管理技术。IBM Storwize V7000 是一个模块化的终端存储产品，能够与需求同步增长。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、注入任意 WEB/HTML 代码或执行任意脚本代码。

CNVD 收录的相关漏洞包括：IBM Global Console Managers 存在未明任意代码执行漏洞、IBM Storwize V7000 Unified 存在未明权限提升漏洞、IBM InfoSphere Master Data Management-Collaborative Edition 跨站脚本漏洞、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2014-04539）、IBM InfoSphere MDM Server for PIM 和 IBM InfoSphere MDM - Collaborative Edition 跨站脚本漏洞、IBM InfoSphere MDM Server for PIM 和 IBM InfoSphere MDM - Collaborative Edition 输入验证漏洞、IBM InfoSphere MDM Server for PIM 和 IBM InfoSphere MDM - Collaborative Edition 信息泄露漏洞、IBM Global Console Managers 跨站脚本漏洞。其中“IBM Global Console Managers 存在未明任意代码执行漏洞、IBM Storwize V7000 Unified 存在未明权限提升

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-2014-04609>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04395>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04592>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04539>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04556>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04567>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04568>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04611>

3、Advantech 产品安全漏洞

Advantech WebAccess HMI/SCADA 是一款 HMI/SCADA 软件。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、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：Advantech WebAccessbwocxrun 不安全 ActiveX 控件信息泄露漏洞、Advantech WebAccess 远程验证绕过漏洞、Advantech WebAccess 密码泄露漏洞、Advantech WebAccess 多个 ActiveX 控件缓冲区溢出漏洞、Advantech WebAccess 远程代码执行漏洞。除“Advantech WebAccess 远程代码执行漏洞”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-2014-04532>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04531>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04530>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04544>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04462>

4、Apache 产品安全漏洞

Apache HTTP Server 是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。Traffic Server 是 Apache 软件基金会所研发的开放源码代理服务器和 Web 缓存服务器。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：Apache HTTP Server 'mod_status'远程执行代码漏洞、Apache HTTP Server mod_cache 模块拒绝服务漏洞、Apache HTTP Server mod_proxy 模块远程拒绝服务漏洞、Apache HTTP Server 远程拒绝服务漏洞（CNVD-2014-04461、CNVD-2014-04460、CNVD-2014-04459）、Apache Traffic Server traffic_shell 不安全临时文件漏洞。其中“Apache HTTP Server 'mod_status'远程执行代码漏洞”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-2014-04392>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04572>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04571>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04461>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04460>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04459>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04519>

5、Embarcadero ER/Studio Data Architect ActiveX 远程代码执行漏洞

Embarcadero ER/Studio Data Architect (ER/Studio DA)是一种可视化数据建模工具。本周，Embarcadero ER/Studio Data Architect 被披露存在综合评级为“高危”的远程代码执行漏洞。攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，触发缓冲区溢出，或使应用程序崩溃、执行任意代码。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/patchInfo/show/47507>

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-2014-04383	Citrix XenServer HVM Graphics 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： https://support.citrix.com/article/CTX141036
CNVD-2014-04381	BitdefenderGravityZone 存在多个漏洞	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.bitdefender.com
CNVD-2014-04391	IPython Notebook 远程代码执行漏洞	高	用户可以联系供应商获得补丁信息： http://ipython.org/notebook.html
CNVD-2014-04434	vBulletin SQL 注入漏洞（NVD-C-2014-18656）	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.vbulletin.com/
CNVD-2014-04443	Claws Mail 插件'sc_html_read_line()'函数内存破坏漏洞	高	用户可以联系供应商获得补丁信息： http://www.claws-mail.org/news.php

CNVD-2014-04456	libicu 'locale_get_display_name()' 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://icu-project.org/index.html
CNVD-2014-04457	PHP 'get_icu_value_internal()' 函数内存破坏漏洞	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.php.net/downloads.php
CNVD-2014-04485	CybozuGaroon CGI 组件操作系统命令注入漏洞	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： http://cs.cybozu.co.jp/information/gr20140421news01.php
CNVD-2014-04481	Raritan PowerIQ 存在多个 SQL 注入漏洞	高	暂无
CNVD-2014-04535	ol-commerce 存在多个漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Mozilla 多款产品披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，可执行任意代码。此外，IBM、Advantech、Apache 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，获取敏感信息或发起拒绝服务攻击。另外，Embarcadero ER/Studio Data Architect 被披露存在一个高危零日漏洞。攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，触发缓冲区溢出，或使应用程序崩溃、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、Autodesk 修补 SketchBook Pro 产品漏洞

Autodesk SketchBook Pro 是一款漂亮的自然绘画软件。

本周，Autodesk 修补了上述产品存在的数据边界和整数溢出漏洞，避免远程攻击者利用漏洞执行任意代码。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/47871>

<http://www.cnvd.org.cn/patchInfo/show/47870>

本周要闻速递

1. XP 再曝 0day 漏洞

最近，国外安全研究人员公布了一个影响 Windows XP 系统的 0day 漏洞。据称该漏洞早在 4 月 28 日已报告微软，但由于 XP 失去微软服务支持而得不到补丁，研究人员根据漏洞信息披露原则在一段时间后公开漏洞细节。据介绍此次曝光的 XP 漏洞主要影响企业用户，该漏洞可被恶意程序利用获得系统控制权，破坏和禁用大多数安全软件，包括反病毒软件、防火墙、主动防御软件、沙箱和还原系统等，也可以用于绕过 Windows 安全保护机制，或者在服务器上提升权限，控制整个网络服务器，直接威胁到政府、企业、网吧的信息安全。

参考链接：<http://www.techweb.com.cn/news/2014-07-23/2058508.shtml>

2. Linux 曝出重大安全漏洞

近日，Linux Kernel 被爆本地权限提升的漏洞。据微博介绍，利用该漏洞，黑客可以成功获取到 Linux 系统的 root 权限。同时，该漏洞在 Red Hat、ubuntu、Debian 等 Linux 系统大部分版本上均可复现。近期也有安全人员表示，利用漏洞已成功取得某 Android 手机的 root 权限。因此，提醒广大 IT 运维人员，及时更新自己的 Linux 服务器系统。

参考链接：<http://www.cctime.com/html/2014-7-23/2014723103387155.htm>

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