

信息安全漏洞周报

2014 年 6 月 16 日-2014 年 6 月 22 日

2014 年第 25 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**中**。

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 151 个，其中高危漏洞 49 个、中危漏洞 89 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 142 个。本周收录的漏洞中，已有 108 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“Zero CMS 'article_id'参数 SQL 注入漏洞”，“Yealink VoIP Phone SIP-T38G 'cgiServer.exe'远程命令执行漏洞”的零日攻击代码，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 151 个漏洞。报送情况如表 1 所示。其中，奇虎 360、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、习科网络安全、High-Tech Bridge Security Research 及多个白帽子向 CNVD 提交了 176 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	124	124
天融信	110	0
启明星辰	110	0
安天实验室	107	0
绿盟科技	98	0
恒安嘉新	71	0
习科网络安全	9	9
CNCERT 贵州分中心	12	12

CNCERT 江西分中心	8	8
CNCERT 湖南分中心	5	5
CNCERT 山西分中心	5	5
CNCERT 福建分中心	1	1
CNCERT 山东分中心	1	1
High-Tech Bridge Security Research	2	2
个人	9	9
报送总计	672	176
录入总计	151（去重）	176

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Yealink、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	Mozilla	11	7%
2	Yealink	7	5%
3	Cisco	6	4%
4	Symantec	5	3%
5	SAP	5	3%
6	IBM	5	3%
7	Juniper Networks	3	2%
8	Linux	3	2%
9	Microsoft	1	1%
10	其他	105	70%

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 151 个漏洞。其中应用程序漏洞 94 个，WEB 应用漏洞 25 个，网络设备漏洞 18 个，操作系统漏洞 6 个，安全产品漏洞 6 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	94
WEB 应用漏洞	25
网络设备漏洞	18
操作系统漏洞	6

安全产品漏洞	6
数据库漏洞	2

表 3 漏洞按影响类型统计表

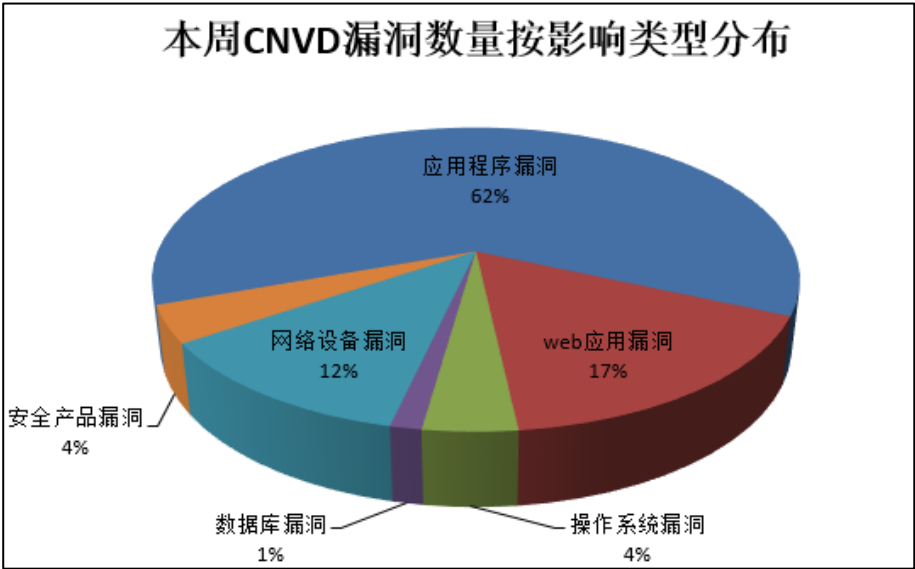


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞，1 个移动互联网，1 个工控行业漏洞（如下图表所示）。其中，“Cisco IOS XR Software IPv6 数据包处理拒绝服务漏洞、多个 Asterisk 产品远程权限提升漏洞、Check Point Security Gateways 存在多个拒绝服务漏洞、Sagem 2604 Router 'password.cgi'密码泄露漏洞”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-2014-03695	Cisco Autonomic Networking Infrastructure 安全绕过漏洞	中	是
电信	CNVD-2014-03690	Apache Tomcat Crafted Request Handling CPU Resource Consumption 远程拒绝服务漏洞	中	是
电信	CNVD-2014-03705	Cisco IOS XR Software IPv6 数据包处理拒绝服务漏洞	高	是
电信	CNVD-2014-03704	Cisco NX-OS 软件 HSRP 数据包解析拒绝服务漏洞	中	否
电信	CNVD-2014-03700	多个 Asterisk 产品远程权限提升漏洞	高	是
电信	CNVD-2014-03712	Huawei Campus Series Switches 堆缓冲区溢出漏洞	中	是
电信	CNVD-2014-03725	Asterisk PJSIP Channel Driver 拒绝服务漏洞	中	是

电信	CNVD-2014-03732	SEIL Series Routers 远程拒绝服务漏洞	中	是
电信	CNVD-2014-03736	Check Point Security Gateways 存在多个拒绝服务漏洞	高	是
电信	CNVD-2014-03745	Sagem 2604 Router 'password.cgi'密码泄露漏洞	高	是
电信	CNVD-2014-03760	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2014-03760)	低	是
电信	CNVD-2014-03776	ZTE ZXV10 W300 RomPager 拒绝服务漏洞	中	否
电信	CNVD-2014-03777	Asterisk Open Source 拒绝服务漏洞 (CNVD-2014-03777)	中	是
电信	CNVD-2014-03784	Juniper Junos 存在多个产品弱加密信息泄露漏洞	中	是
电信	CNVD-2014-03801	OpenStack Neutron L3 Router IPv6 子网拒绝服务漏洞	中	是
移动互联网	CNVD-2014-03808	050 plus for Android 信息泄露漏洞	低	是
工控系统	CNVD-2014-03746	Parallels Plesk Panel XML 外部实体注入漏洞	中	否

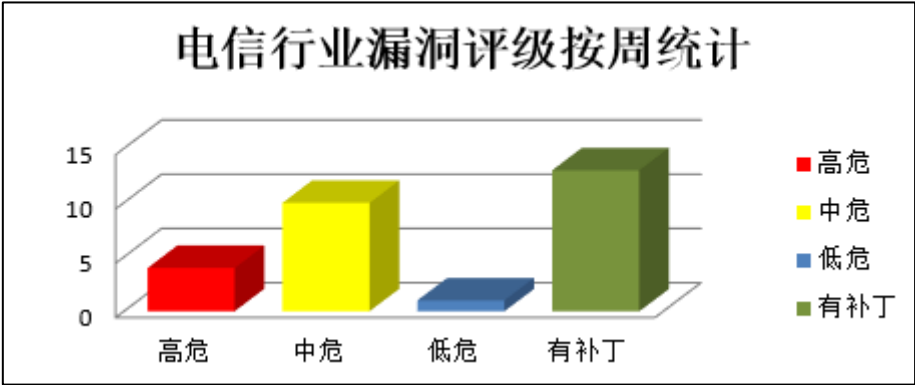


图 1 电信行业漏洞统计

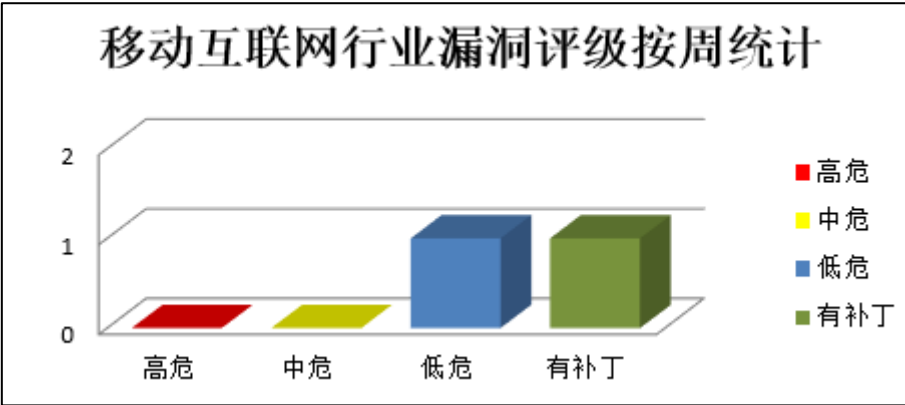


图 2 移动互联网行业漏洞统计

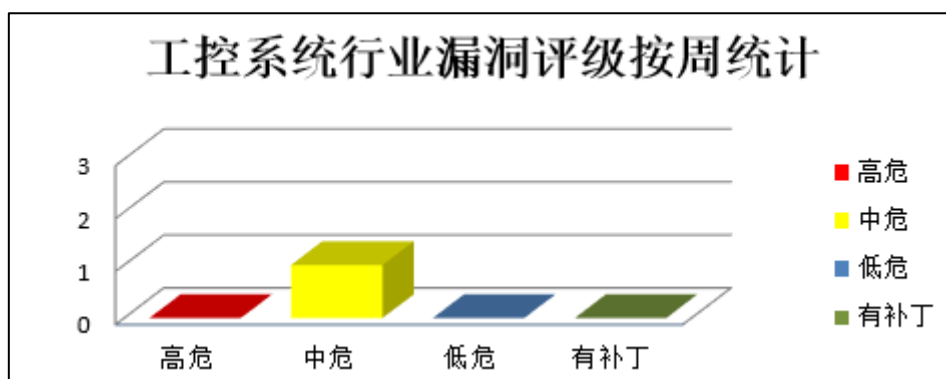


图 3 工控行业漏洞统计

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、Symantec 产品安全漏洞

Symantec Web Gateway 提供了网络内容过滤和的数据泄露防护功能。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞在受影响站点的用户浏览器中执行任意脚本代码或进行未授权操作。

CNVD 收录的相关漏洞包括：Symantec Web Gateway 'SNMPConfig.php'远程命令执行漏洞、Symantec Web Gateway 存在多个跨站脚本漏洞、Symantec Web Gateway 'SNMPConfig.php'远程命令注入漏洞、Symantec Web Gateway SQL 注入漏洞（CNVD-2014-03718、CNVD-2014-03719）。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-2014-03796>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03716>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03717>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03718>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03719>

2、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/邮件客户端。本周，上述产品被披露存在内存错误引用和缓冲区溢出漏洞，攻击者可利用漏洞构建特制 WEB 页，诱使用户解析，可使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird SMIL 动画控制器内存错误引用漏洞、Mozilla Firefox event listener 管理程序内存错误引用漏洞、Mozilla Firefox Gamepad API 缓冲区溢出漏洞、Mozilla Firefox nsTextEditRules::CreateMozBR 内存错误引用漏洞、Mozilla Firefox mozilla::dom::workers::WorkerPrivateParent 内存错误引

用漏洞。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-2014-03666>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03669>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03668>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03671>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03672>

3、DotNetNuke 产品安全漏洞

DotNetNuke 是一款开源的内容管理系统。本周，上述产品被披露存在任意文件下载漏洞，攻击者可利用漏洞提交特殊的 URL 请求下载任意文件。

CNVD 收录的相关漏洞包括：DotNetNukeResponsiveSidebar 'ResponsiveSidebarDownload.aspx'任意文件下载漏洞、DotNetNukeEventsCalendar 'downloadaddoc.aspx'任意文件下载漏洞、DotNetNukeEasyDnnGallery 'ImageDownload.aspx'任意文件下载漏洞、DotNetNukeCodeEditor 'NNCodeEditorDownload.aspx'任意文件下载漏洞。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-2014-03676>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03678>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03679>

4、Juniper Networks 产品安全漏洞

Juniper Networks JUNOS 是一款 Juniper 网络公司的系列边界路由器等所运行的操作系统。Juniper Networks NetScreen Firewall products with ScreenOS 是美国瞻博网络（Juniper Networks）公司的一套运行于 NetScreen 系列防火墙中的操作系统。本周，上述产品被披露存在信息泄露和拒绝服务漏洞，攻击者可利用漏洞获取敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Juniper Junos 存在多个产品弱加密信息泄露漏洞、Juniper Networks NetScreen Firewall products with ScreenOS 拒绝服务漏洞（CNVD-2014-03681、CNVD-2014-03682）。其中，除“Juniper Junos 存在多个产品弱加密信息泄露漏洞”外，其余漏洞的综合评级为“高危”。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-2014-03784>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03681>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03682>

5、Oracle Database 存在多个未明远程代码执行漏洞

Oracle Database 是一款商业性质的大型数据库。本周，Oracle Database 被披露存在综合评级为“高危”的远程代码执行漏洞。攻击者可以利用漏洞绕过安全限制执行 Java 代码，或提升权限等。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-2014-03771>

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-2014-03662	SpiceWorks 存在多个脚本注入漏洞	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.spiceworks.com/
CNVD-2014-03659	WebTitan 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.webtitan.com
CNVD-2014-03686	Kolibri 栈缓冲区溢出漏洞（CNVD-2014-03686）	高	暂无
CNVD-2014-03685	JOAL 'OpenAL32.dll'远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://jogamp.org/
CNVD-2014-03684	AlienVault OSSIM 远程代码执行漏洞（CNVD-2014-03684）	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://forums.alienvault.com/discussion/2690
CNVD-2014-03683	AlienVault OSSIM 远程代码执行漏洞（CNVD-2014-03683）	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://forums.alienvault.com/discussion/2690
CNVD-2014-03680	Kolibri 栈缓冲区溢出漏洞（CNVD-2014-03680）	高	暂无
CNVD-2014-03697	WordPress Felici Theme 'uploadify.php'任意文件上传漏洞	高	暂无
CNVD-2014-03713	ScrumWorks Pro Administrator Password Reset 安全绕过漏洞	高	暂无
CNVD-2014-03730	多个 Puppet 产品远程代码执行漏洞	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： http://puppetlabs.com/security

表 3 部分高危漏洞列表

小结：本周，Symantec 产品被披露存在多个漏洞，攻击者可利用漏洞在受影响站点的用户浏览器中执行任意脚本代码或进行未经授权操作。此外，Mozilla、DotNetNuke、Juniper Networks 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，下载任意文件、获取敏感信息或发起拒绝服务攻击。另外，Oracle Database 被披露存在一个高危零日漏洞。攻击者可以利用漏洞绕过安全限制执行 Java 代码，或提升权限等。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、Microsoft 修补 Malware Protection Engine 产品漏洞

Microsoft 恶意软件保护引擎(Malware Protection Engine) 是微软推出用以侦测恶意程式软体的防护引擎。

本周，Microsoft 修补了上述产品存在的拒绝服务漏洞，避免攻击者可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/46602>

本周要闻速递

1. Google Play 出现安全漏洞

日前，哥伦比亚大学计算机科学教授 Jason Nieh 和博士生 Nicolas Viennot 在所进行的研究中发现，Google Play 中存有一个非常严重的安全漏洞，它将让用户的数据受到威胁，甚至还可能殃及所有的 Android 软件。现在，谷歌已经跟这两位研究人员开始着手寻找解决该漏洞的方法。目前还不清楚该漏洞是否会影响到软件第三方登陆的端口。而谷歌正在使用 PlayDrone 全面扫描 Google Play 中的软件。

参考链接：http://tech.ifeng.com/google/detail_2014_06/20/36931422_0.shtml

2. 微软安全软件发现危险漏洞

北京时间 6 月 20 日消息，据外媒报道，微软本周发布安全警报，并推出一个紧急补丁以修复其软件中的一个危险漏洞。据悉，这个漏洞牵涉的范围太广，涵盖了微软 Windows 系统中的免费杀毒软件 Microsoft Security Essentials、企业安全产品 Forefront 以及微软一直在大力向企业用户推广的安全云服务 Intune 等。

参考链接：<http://news.zol.com.cn/461/4619575.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