

信息安全漏洞周报

2015 年 03 月 16 日-2015 年 03 月 22 日

2015 年第 12 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 164 个，其中高危漏洞 60 个、中危漏洞 88 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 144 个。本周收录的漏洞中，已有 137 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“724 CMS SQL 'ID'参数 SQL 注入漏洞”、“Betster 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 家成员单位及个人报送了本周收录的全部 164 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、恒安嘉新等单位报送数量较多。此外，补天平台、CNCERT 各分中心、习科网络安全、深圳市深信服电子科技有限公司及白帽子向 CNVD 提交了 953 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	903	903
天融信	121	9
启明星辰	108	0
安天实验室	103	0
恒安嘉新	82	0
绿盟科技	32	0

习科网络安全	2	2
深圳市深信服电子科技有限公司	1	1
CNCERT 宁夏分中心	9	9
CNCERT 福建分中心	6	6
CNCERT 陕西分中心	3	3
个人	20	20
报送总计	1390	953
录入总计	164（去重）	953

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Drupal 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	Microsoft	23	14%
2	IBM	17	10%
3	Apple	17	10%
4	Adobe	11	7%
5	Cisco	9	5%
6	WordPress	8	5%
7	EMC	5	3%
8	MyBB	5	3%
9	Linux	4	2%
10	其他	65	41%

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 164 个漏洞。其中应用程序漏洞 117 个，WEB 应用漏洞 30 个，操作系统漏洞 12 个，网络设备漏洞 4 个，安全产品 1 个。

漏洞影响对象类型	漏洞数量
----------	------

应用程序漏洞	117
WEB 应用漏洞	30
操作系统漏洞	12
网络设备漏洞	4
安全产品漏洞	1

表 3 漏洞按影响类型统计表

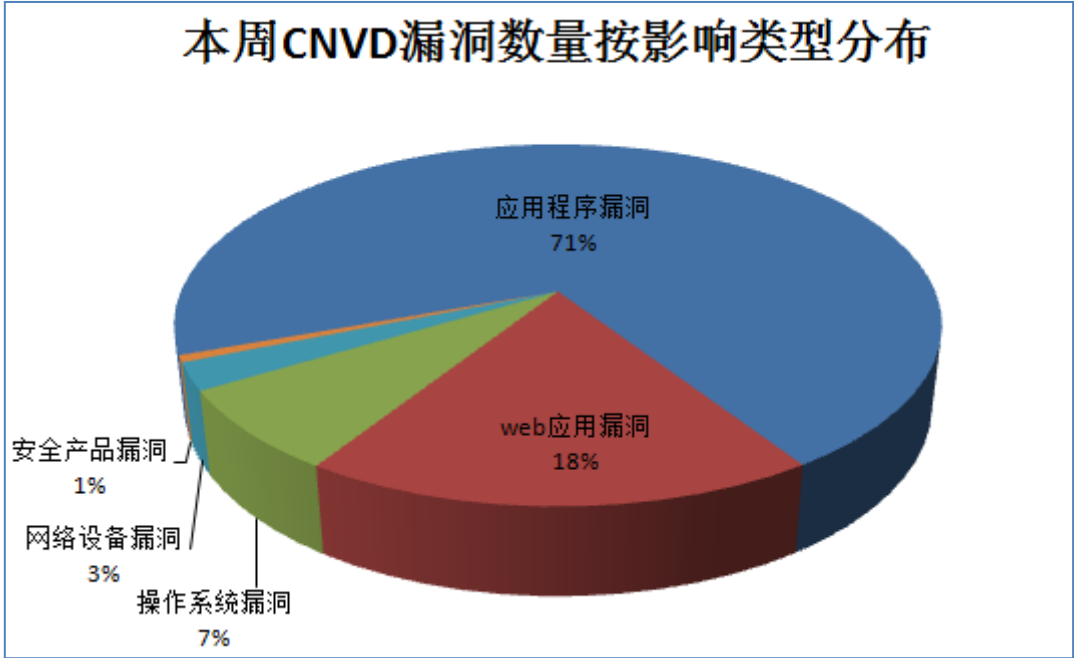


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 个电信行业漏洞，2 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图表所示）。其中，“Cisco AnyConnect Secure Mobility Client 权限提升漏洞、Android media 整数溢出漏洞”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-2015-01721	IBM WebSphere 跨站请求伪造漏洞	中	是
电信	CNVD-2015-01720	IBM WebSphere Commerce XML 外部实体引用敏感信息泄露漏洞	中	是
电信	CNVD-2015-01812	MikroTik RouterOS 跨站请求伪造漏洞	中	否
电信	CNVD-2015-01833	Cisco AnyConnect Secure Mobility Client 权限提升漏洞	高	是
电信	CNVD-2015-01832	Cisco AnyConnect Secure Mobility Client 任意文件写漏洞	中	是
电信	CNVD-2015-01831	Cisco AnyConnect Secure Mobility Client Hostscan 路径遍历漏洞	中	是

电信	CNVD-2015-01843	Cisco Content Services Switch 安全限制绕过漏洞	中	否
电信	CNVD-2015-01868	Cisco AnyConnect Secure Mobility Client 任意代码执行漏洞 (CNVD-2015-01868)	中	否
移动互联网	CNVD-2015-01829	Android media 整数溢出漏洞	高	是
移动互联网	CNVD-2015-01874	Android audio_policy app 本地应用拒绝服务漏洞	低	是
工控系统	CNVD-2015-01826	Cimon CmnView DLL 劫持漏洞	中	是
工控系统	CNVD-2015-01834	Honeywell XL Web Controller 目录遍历漏洞	高	否

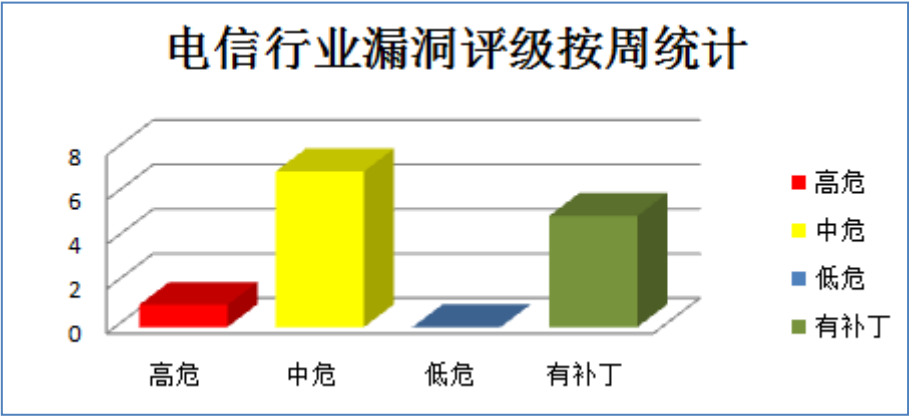


图 1 电信行业漏洞统计

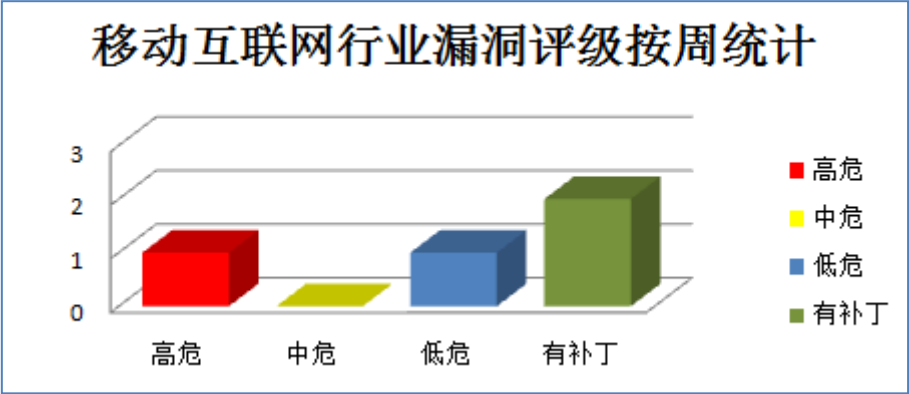


图 2 移动互联网行业漏洞统计

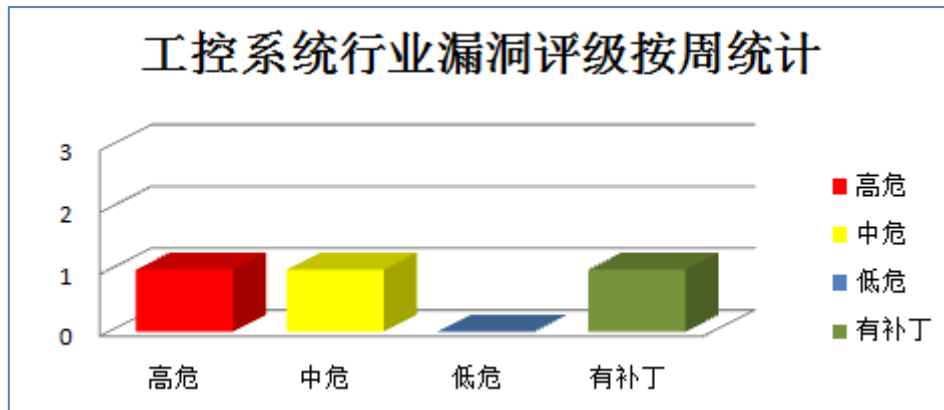


图 3 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一个流行的 WEB 浏览器。本周，上述产品被披露存在内存破坏和权限提升漏洞，攻击者可利用漏洞提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft IE 内存破坏漏洞（CNVD-2015-01677、CNVD-2015-01682、CNVD-2015-01681、CNVD-2015-01680、CNVD-2015-01679、CNVD-2015-01684、CNVD-2015-01683）、Microsoft IE 权限提升漏洞。其中，除“Microsoft IE 权限提升漏洞”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-2015-01677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01682>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01681>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01680>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01679>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01684>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01683>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01678>

2、Adobe 产品安全漏洞

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。本周，上述产品被披露存在任意代码执行和内存错误引用漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 任意代码执行漏洞（CNVD-2015-01802、CNVD-2015-01801、CNVD-2015-01800、CNVD-2015-01799、CNVD-2015-01798、CNVD-2015-01797）、Adobe Flash Player 内存错误引用漏洞（CNVD-2015-01807、CNVD-2015-01806）。上述漏洞的综合评级为“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-2015-01802>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01801>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01800>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01799>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01798>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01797>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01807>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01806>

3、WebKit 安全漏洞

WebKit 是开源的 Web 浏览器引擎，目前被 Safari、Chrome 等浏览器使用。本周，上述产品被披露存在内存破坏漏洞，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：Apple Safari WebKit 内存破坏漏洞（CNVD-2015-01848、CNVD-2015-01849、CNVD-2015-01850、CNVD-2015-01851、CNVD-2015-01852、CNVD-2015-01853、CNVD-2015-01854、CNVD-2015-01855）。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-2015-01848>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01849>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01850>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01851>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01852>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01853>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01854>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01855>

4、IBM 产品安全漏洞

IBM Rational DOORS Next Generation 和 Rational Requirements Composer 都是美国 IBM 公司的需求管理解决方案。该方案主要用于定义、管理和报告项目生命周期中的需求。IBM Rational Jazz Team Server (JTS) 是美国 IBM 公司的一套基于 IBM Rational 新一代产品的 Java 协作平台。该平台被封装为一个 Web 存档文件（WAR 文件），

伴随 Rational Team Concert 1.0 (RTC1.0) 一同发布，可部署在应用服务器上为 RTC 提供底层 Web 服务。IBM Rational Quality Manager 是一个协作的、基于 Web 的质量管理解决方案。本周，上述产品被披露存在拒绝服务、信息泄露和跨站脚本漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Rational DOORS Next Generation 和 Rational Requirements Composer 拒绝服务漏洞、IBM Rational DOORS Next Generation 和 Rational Requirements Composer 跨站脚本漏洞、IBM Rational Jazz Team Server 信息泄露漏洞、IBM Rational Jazz Team Server 任意用户仪表盘删除漏洞、IBM Rational Quality Manager 跨站脚本漏洞 (CNVD-2015-01712、CNVD-2015-01711、CNVD-2015-01710、CNVD-2015-01709)。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-2015-01870>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01871>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01872>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01873>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01712>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01711>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01710>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01709>

5、Comsenz SupeSite CMS SQL 注入漏洞

Comsenz SupeSite 7.0 CMS 是一款康盛开发的内容管理系统。本周，Comsenz SupeSite CMS 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用该漏洞提交特制的 SQL 查询，操作或获取数据库数据。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-2015-01875>

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-2015-01673	Xen 存在多个漏洞	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://xenbits.xen.org/xsa/advisory-123.html
CNVD-2015-01687	BACnet OPC Server 堆缓冲区溢出漏洞	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.scadaengine.com/downloads/BACnetOPCServer_2.1.371.24.exe

CNVD-2015-01686	BACnet OPC Server 身份验证漏洞	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.scadaengine.com/downloads/BACnetOPCServer_2.1.371.24.exe
CNVD-2015-01699	pngcrush 远程代码执行漏洞	高	pngcrush v1.7.84 已经修复该漏洞，建议用户下载更新： http://sourceforge.net/p/pmt/news/2015/02/pngcrush-1784-released/
CNVD-2015-01701	WebGate eDVR Manager 存在多个缓冲区溢出漏洞	高	暂无
CNVD-2015-01688	DRAM 'Rowhammer'内存位翻转权限提升漏洞	高	暂无
CNVD-2015-01695	Foxit Reader GIF 文件 LZWMini mumCodeSize 内存破坏漏洞	高	Foxit Reader 7.1 已经修复该漏洞，建议用户下载更新： http://www.foxitsoftware.com/support/security_bulletins.php#FRD-25
CNVD-2015-01696	Foxit Reader GIF 文件 Ubyte 字节处理内存破坏漏洞	高	Foxit Reader 7.1 已经修复该漏洞，建议用户下载更新： http://www.foxitsoftware.com/support/security_bulletins.php#FRD-25
CNVD-2015-01703	WebGate Control Center 多个控件缓冲区溢出漏洞	高	暂无
CNVD-2015-01724	WordPress 插件 Huge IT Slider S QL 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： https://wordpress.org/support/topic/huge-it-slider-security-vulnerability-notification-sql-injection

表 3 部分高危漏洞列表

小结：本周，Microsoft Internet Explorer 被披露存在内存破坏和权限提升漏洞，攻击者可利用漏洞提升权限或执行任意代码。此外，Adobe、WebKit、Apple 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞进行跨站攻击、执行任意代码或发起拒绝服务攻击。另外，Comsenz SupeSite CMS 被披露存在一个高危零日漏洞，攻击者可利用该漏洞提交特制的 SQL 查询，操作或获取数据库数据。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、Google 修补 Chrome 产品漏洞

Google Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具。

本周，Google 修补了上述产品存在信息泄露漏洞，避免攻击者利用漏洞通过 web 站点触发 ondevicemotion 事件。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/56319>

<http://www.cnvd.org.cn/patchInfo/show/56321>



本周要闻速递

1. 苹果 Mac OS X 系统被发现存在 DLL 劫持漏洞

本周，Synack 的研究员 Patrick Wardle 在温哥华举行的 CanSecWest 的会议上做了一个演讲，他详细解释了入侵 Mac OS X 动态库的细节：持久、过程注入、安全功能（Apple Gatekeeper）绕过和远程利用，和 Windows DLL 劫持差不多。DLL 劫持攻击和动态库劫持攻击的概念从本质上来说基本相同：攻击者必须先找到一个恶意库，然后才能进入操作系统加载的目录中。Wardle 只是解释了这类攻击的一个方面，也就是他能找到 Photostream Agent（iCloud 运行时会自动运行）上易受攻击的 Apply 二进制文件。

参考链接：<http://www.freebuf.com/news/61244.html>

2. 一种强大的新型 BIOS Bootkit 病毒曝光

近日，安全研究人员开发出一种新的 BIOS bootkit，它可以窃取敏感数据，以及流行操作系统使用的 PGP 密钥。包括华硕、惠普、宏基、技嘉以及微星等在内的各大供应商的主板都受到该病毒影响。BIOS bootkits 是真实存在的。斯诺登在披露 NSA ANT 部门使用的监视工具集时，曾提到过 BIOS bootkits。这些恶意软件能够入侵受害机器的 BIOS，以此确保隐藏的持久性以及实现复杂的逃避技术。即使重装操作系统，BIOS bootkits 仍然能够存留。

参考链接：<http://www.freebuf.com/news/61478.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