

信息安全漏洞周报

2015 年 01 月 12 日-2015 年 01 月 18 日

2015 年第 3 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 170 个，其中高危漏洞 61 个、中危漏洞 102 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 156 个。本周收录的漏洞中，已有 109 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“WordPress 插件 AJAX Post Search 'the_search_function' SQL 注入漏洞”、“Kofax e-Transactions Sender Sendbox 文件注入漏洞”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、合作伙伴及个人报送了本周收录的全部 170 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、启明星辰、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 1146 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	1132	1132
安天实验室	141	0
启明星辰	117	0
天融信	109	0

恒安嘉新	100	0
绿盟科技	57	0
High-Tech Bridge Security Research Lab	1	1
CNCERT 福建分中心	3	3
CNCERT 河南分中心	3	3
CNCERT 山西分中心	1	1
个人	6	6
报送总计	1670	1146
录入总计	170（去重）	1146

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco 、WordPress、Mozilla 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	Cisco	13	8%
2	WordPress	12	7%
3	Mozilla	10	6%
4	Adobe	9	5%
5	OpenSSL	9	5%
6	Microsoft	8	5%
7	Drupal	8	5%
8	Wireshark	6	4%
9	VDG Security BV	6	4%
10	其他	89	51%

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 170 个漏洞。其中应用程序漏洞 96 个，WEB 应用漏洞 55 个，操作系统漏洞 11 个，网络设备漏洞 7 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
----------	------

应用程序漏洞	96
WEB 应用漏洞	55
操作系统漏洞	11
网络设备漏洞	7
安全产品漏洞	1

表 3 漏洞按影响类型统计表

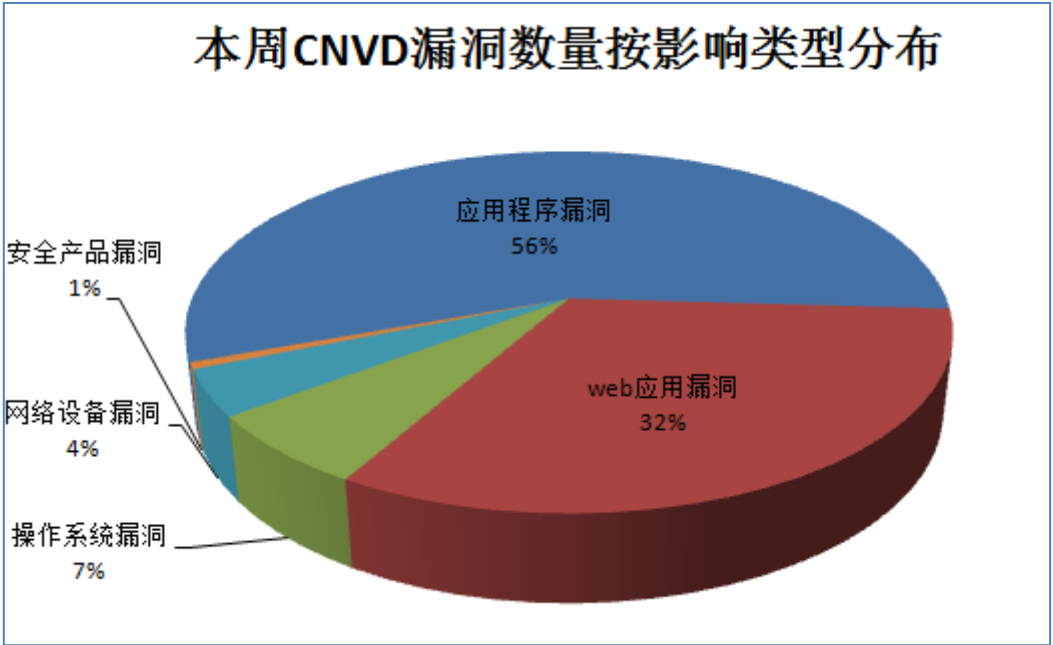


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 14 个电信行业漏洞， 1 个移动互联网行业漏洞（如下图表所示）。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-00233	Cisco WebEx Meetings Server 跨站请求伪造漏洞（CNVD-2015-00233）	中	是
电信	CNVD-2015-00232	Cisco Secure Access Control Server 权限提升漏洞	中	是
电信	CNVD-2015-00231	Cisco WebEx Meetings Server 跨站脚本漏洞	中	是
电信	CNVD-2015-00230	Cisco Secure Access Control Server 存在多个跨站脚本漏洞（CNVD-2015-00230）	中	是
电信	CNVD-2015-00229	Cisco WebEx Meetings Server 加密密码泄露漏洞	中	是
电信	CNVD-2015-00228	Cisco Secure Access Control Server 开放重定向漏洞	中	是

电信	CNVD-2015-00227	Cisco WebEx Meetings Server 验证绕过漏洞	中	是
电信	CNVD-2015-00225	Cisco WebEx Meetings Server 用户枚举漏洞 (CNVD-2015-00225)	中	是
电信	CNVD-2015-00223	Cisco MDS 9000 NX-OS Software 拒绝服务漏洞	中	是
电信	CNVD-2015-00224	Cisco WebEx Meetings Server 用户枚举漏洞 (CNVD-2015-00224)	中	是
电信	CNVD-2015-00239	Cisco WebEx Meetings Server 存在未明漏洞	中	是
电信	CNVD-2015-00277	Cisco WebEx Meetings Server 信息泄露漏洞 (CNVD-2015-00277)	中	是
电信	CNVD-2015-00289	ZTE MF19 存在多个漏洞	高	否
电信	CNVD-2015-00301	discuz!本地文件包含漏洞	高	否
移动互联网	CNVD-2015-00290	多个 BlackBerry 产品本地安全绕过漏洞	中	是

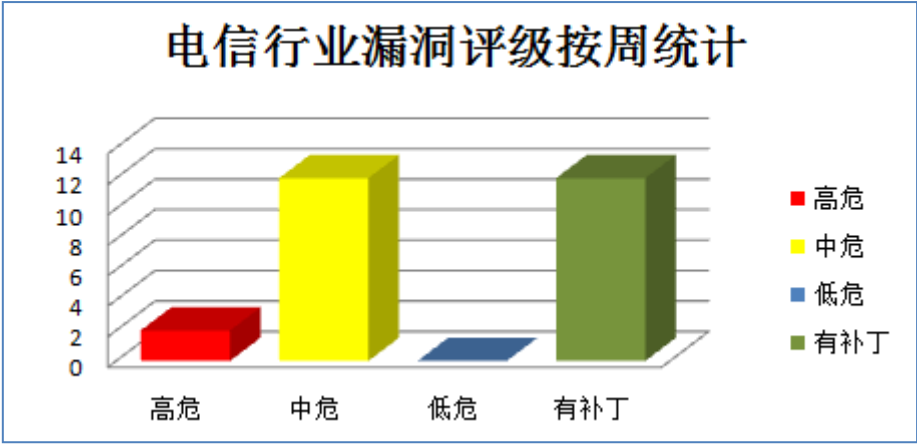


图 1 电信行业漏洞统计

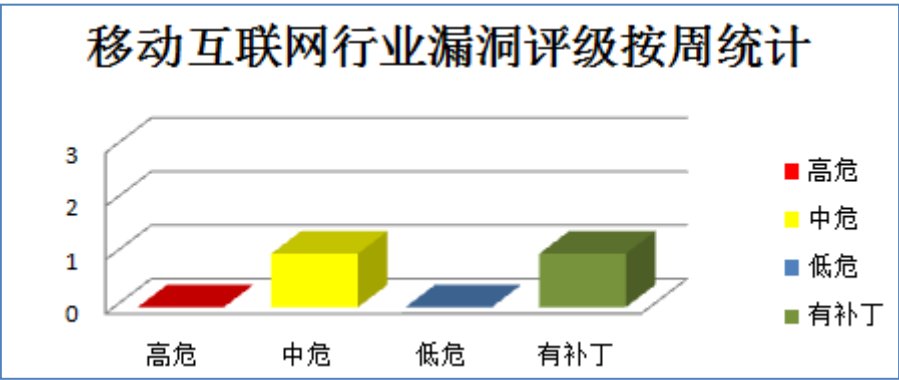


图 2 移动互联网行业漏洞统计

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

1 月 13 日，微软发布了 2015 年 1 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows 中存在的 8 个安全漏洞。其中，1 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，进行拒绝服务攻击。CNVD 提醒广大 Microsoft 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。

CNVD 收录的相关漏洞包括：Microsoft Windows Server 本地权限提升漏洞、Microsoft Windows 本地权限提升漏洞（CNVD-2015-00360）、Microsoft Windows 错误报告安全机制绕过漏洞、Microsoft Windows Telnet 服务缓冲区溢出漏洞、Microsoft Windows Kernel 'mrxdav.sys'本地权限提升漏洞、Microsoft Windows Server DNS 和 LDAP 响应欺骗漏洞、Microsoft Windows TS WebProxy Windows 远程权限提升漏洞、Microsoft Windows Network Policy Server 远程拒绝服务漏洞。其中，除“Microsoft Windows 错误报告安全机制绕过漏洞、Microsoft Windows Kernel 'mrxdav.sys'本地权限提升漏洞、Microsoft Windows Server DNS 和 LDAP 响应欺骗漏洞”外，其余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/webinfo/show/3565>

2、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，攻击者可利用漏洞获取敏感信息、进行未授权操作、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 存在多个内存破坏漏洞（CNVD-2015-00362、CNVD-2015-00363）、Mozilla Firefox/SeaMonkey Web RTC 内存破坏漏洞、Mozilla Firefox Gecko Media 插件沙盒绕过漏洞、Mozilla Firefox/SeaMonkey XrayWrapper 权限提升漏洞、Mozilla Firefox/SeaMonkey 位图呈现信息泄露漏洞、Mozilla Firefox/Thunderbird/SeaMonkey sendBeacon 跨站请求伪造漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 代理验证会话固定漏洞。其中，除“Mozilla Firefox/SeaMonkey 位图呈现信息泄露漏洞、Mozilla Firefox/Thunderbird/SeaMonkey sendBeacon 跨站请求伪造漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 代理验证会话固定漏洞”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-2015-00362>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00363>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00368>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00369>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00371>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00364>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00365>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00366>

3、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。Adobe Air 是一款 Adobe 公司出品的跨操作系统的运行时库。本周，上述产品被披露存在内存破坏、缓冲区溢出、信息泄露和远程代码漏洞，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：Adobe Flash Player and AIR 存在未明内存破坏漏洞（CNVD-2015-00340、CNVD-2015-00335）、Adobe Flash Player and AIR 存在未明堆缓冲区溢出漏洞（CNVD-2015-00339、CNVD-2015-00333）、Adobe Flash Player and AIR 远程代码执行漏洞（CNVD-2015-00338、CNVD-2015-00332）、Adobe Flash Player and AIR 信息泄露漏洞（CNVD-2015-00336）、Adobe Flash Player and AIR 越界读取内存破坏漏洞。其中，除“Adobe Flash Player and AIR 信息泄露漏洞（CNVD-2015-00336）”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-2015-00340>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00335>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00339>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00333>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00338>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00332>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00336>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00334>

4、Cisco 产品安全漏洞

Cisco WebEx Meetings 是网络会议解决方案。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、执行未经授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括：Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2015-00277）、Cisco WebEx Meetings Server 存在未明漏洞、Cisco WebEx Meetings Server 用户枚举漏洞（CNVD-2015-00224、CNVD-2015-00225）、Cisco WebEx Meetings Server 验证绕过漏洞、Cisco WebEx Meetings Server 加密密码泄露漏洞、Cisco WebEx Meetings Server 跨站脚本漏洞、Cisco WebEx Meetings Server 跨站请求伪造漏洞（CNVD-2015-00233）。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-2015-00277>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00239>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00224>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00225>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00227>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00229>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00231>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00233>

5、ProjectSend 任意文件上传漏洞

ProjectSend 是一套基于 PHP 和 MySQL 的自托管应用程序。本周, ProjectSend 被披露存在综合评级为“高危”的任意文件上传漏洞。攻击者可以利用漏洞执行任意 PHP 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/flaw/show/CNVD-2015-00382>

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-2015-00196	Zabbix 'chart_bar.php'存在多个 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: https://support.zabbix.com/browse/ZBX-8582
CNVD-2015-00195	Installatron GQ File Manager SQL 注入漏洞	高	暂无
CNVD-2015-00197	Mini-stream RM-MP3 Converter 缓冲区溢出漏洞 (CNVD-2015-00197)	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://www.exploit-db.com/exploits/35377
CNVD-2015-00218	WordPress 插件 Cdnvote SQL 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://wpsecure.net/2011/02/cdnvote-plugin/ https://plugins.trac.wordpress.org/changeset/350873/cdnvote/trunk/cdnvote-post.php
CNVD-2015-00219	Redaxscript 'includes/password.php'存在多个 SQL 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: https://www.htbridge.com/advisory/

			HTB22804
CNVD-2015-00238	WordPress 插件 Shopping Cart 'banneruploaderscript.php'任意文件上传漏洞	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://wordpress.org/plugins
CNVD-2015-00234	TYPO3 Content Rating SQL 注入漏洞	高	暂无
CNVD-2015-00236	TYPO3 Content Rating Extbase Extension 存在多个输入验证漏洞	高	暂无
CNVD-2015-00248	Gogago YouTube Video Converter 缓冲区溢出漏洞	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.gogago.com/
CNVD-2015-00269	Privoxy 存在多个远程代码执行漏洞	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://www.privoxy.org/

表 3 部分高危漏洞列表

小结：1月13日，微软发布了2015年1月份的月度例行安全公告，共含8项更新，修复了Microsoft Windows中存在的8个安全漏洞。其中，1项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，进行拒绝服务攻击。CNVD提醒广大Microsoft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。此外，Mozilla、Adobe、Cisco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、执行未授权操作、进行跨站攻击或执行任意代码。另外，ProjectSend被披露存在一个高危零日漏洞。攻击者可以利用漏洞执行任意PHP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、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安全绕过和信息泄露漏洞，避免攻击者利用漏洞绕过安全限制和获取敏感信息。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/53939>



本周要闻速递

1. 谷歌再曝 Windows8.1 漏洞

在微软还未来得及发布漏洞补丁时，谷歌 Project Zero 小组再次公布了 Windows8.1 系统的又一新漏洞，该漏洞可导致权限提升。短短几周，这已经是谷歌精英团队公布的有关 Windows8.1 系统的第二个漏洞了。根据谷歌的漏洞公布策略，谷歌是在等待了 90 天之后才公布了此漏洞的细节信息。不过令人好奇的是，在去年 11 月份，微软请求谷歌推迟漏洞公布日期，理由是他们打算在 2015 年 2 月份修复该漏洞。但是，谷歌拒绝了微软的请求，理由是这不符合他们的漏洞公布策略。于是微软决定在 2015 年 1 月修复该漏洞，但谷歌仍旧拒绝推迟该漏洞的公布，即使推迟 2 天也不行。

参考链接：<http://www.freebuf.com/news/56474.html>

2. 微软修复 8 个安全漏洞，包括谷歌披露的 0day 漏洞

微软日前发布了最新安全补丁，修复内容包括谷歌 90 天前提交的 0day 漏洞（微软本计划 2 月修复，但迫于谷歌不愿违背其 90 天公布漏洞详情的策略只好提前发布补丁）等 8 个安全漏洞。其中 Windows Telnet 服务远程代码执行漏洞被微软标记为了高危级别，其余 7 个都是重要级别。此次补丁修复日还修复了另外 3 个特权提升漏洞，2 个安全功能绕过漏洞，一个拒绝服务漏洞。

参考链接：<http://www.freebuf.com/news/56528.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