

信息安全漏洞周报

2015 年 03 月 09 日-2015 年 03 月 15 日

2015 年第 11 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 66 个、中危漏洞 84 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 145 个。本周收录的漏洞中，已有 122 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“PHP MoAdmin 'moadmin.php'远程代码执行漏洞”、“WordPress Photocrati 主题 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、合作伙伴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、安天实验室、天融信、启明星辰、恒安嘉新等单位报送数量较多。此外，补天平台、CNCERT 各分中心、上海天泰网络技术有限公司及白帽子向 CNVD 提交了 934 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	923	923
安天实验室	188	0
天融信	142	0
启明星辰	139	0
恒安嘉新	94	0
绿盟科技	28	0

High-Tech Bridge Security Research Lab	1	1
上海天泰网络技术有限公司	1	1
CNCERT 甘肃分中心	3	3
CNCERT 宁夏分中心	1	1
个人	5	5
报送总计	1525	934
录入总计	164（去重）	934

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	Google	22	13%
2	Microsoft	21	13%
3	Drupal	10	6%
4	HP	10	6%
5	Apple	8	5%
6	WordPress	8	5%
7	Cisco	6	4%
8	Webgate	5	3%
9	IBM	3	2%
10	其他	71	43%

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 94 个，WEB 应用漏洞 38 个，操作系统漏洞 24 个，网络设备漏洞 8 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	38

操作系统漏洞	24
网络设备漏洞	8

表 3 漏洞按影响类型统计表

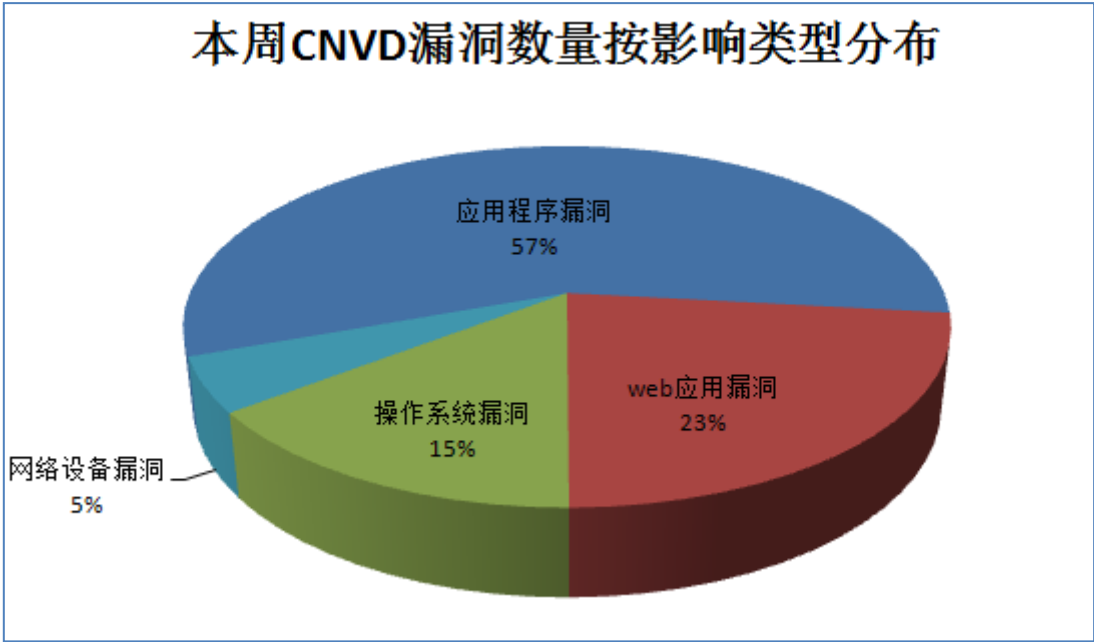


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞，7 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，“Apple iOS SMS 消息空指针引用漏洞、Apple iOS IOSurface 类型混淆漏洞、MICROSYS PROMOTIC 缓冲区溢出漏洞”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-2015-01489	D-Link DIR-636L 存在多个漏洞	高	否
电信	CNVD-2015-01495	Cisco IOS 和 IOS XE RADIUS 实现拒绝服务漏洞	中	是
电信	CNVD-2015-01496	Cisco IOS Authentication Proxy 功能存在未明漏洞	中	是
电信	CNVD-2015-01497	Cisco IOS XR 拒绝服务漏洞（CNVD-2015-01497）	中	是
电信	CNVD-2015-01498	Cisco IOS Autonomic Networking Infrastructure 功能存在未明漏洞	中	是
电信	CNVD-2015-01499	Cisco IOS XR SNMPv2 实现拒绝服务漏洞	中	是
移动互联网	CNVD-2015-01604	多款 Apple 产品存在信息泄露漏洞	中	是
移动互联网	CNVD-2015-01638	Apple iOS 安全绕过漏洞	低	是

移动互联网	CNVD-2015-01637	Apple iOS SMS 消息空指针引用漏洞	高	是
移动互联网	CNVD-2015-01647	多款 Apple 产品 Secure Transport 存在未明漏洞	中	是
移动互联网	CNVD-2015-01641	Apple iOS iCloud Keychain 缓冲区溢出漏洞	中	是
移动互联网	CNVD-2015-01640	Apple iOS IOSurface 类型混淆漏洞	高	是
移动互联网	CNVD-2015-01639	Apple iOS 磁盘挂接逻辑漏洞	中	是
工控系统	CNVD-2015-01544	MICROSYS PROMOTIC 缓冲区溢出漏洞	高	是
工控系统	CNVD-2015-01603	Siemens 多款产品存在搜索路径漏洞	中	是

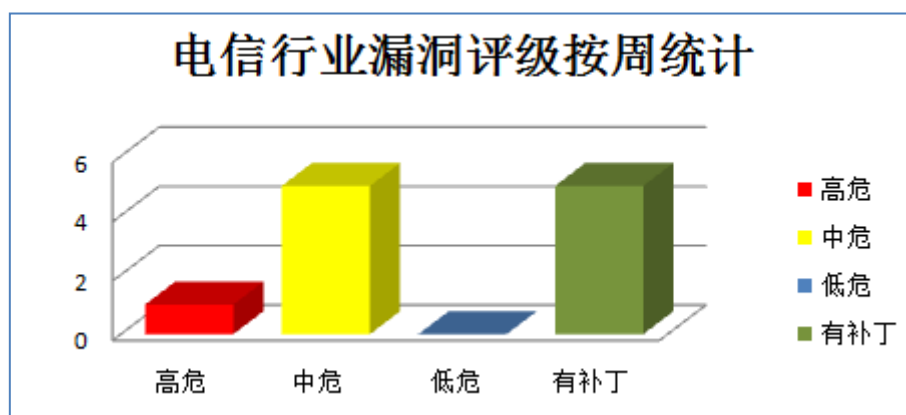


图 1 电信行业漏洞统计

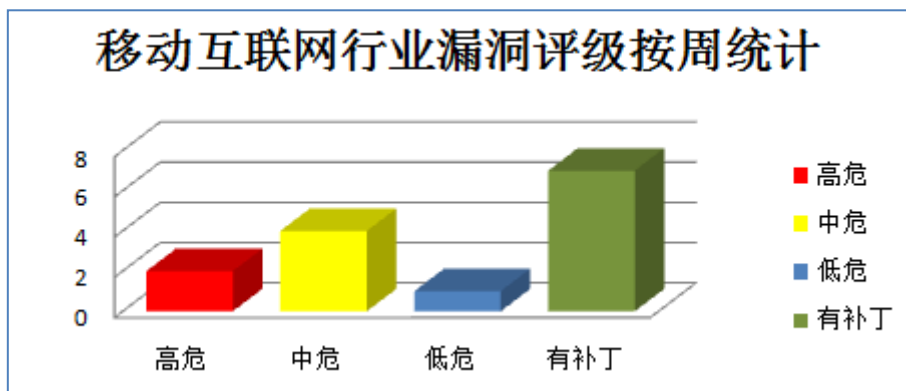


图 2 移动互联网行业漏洞统计

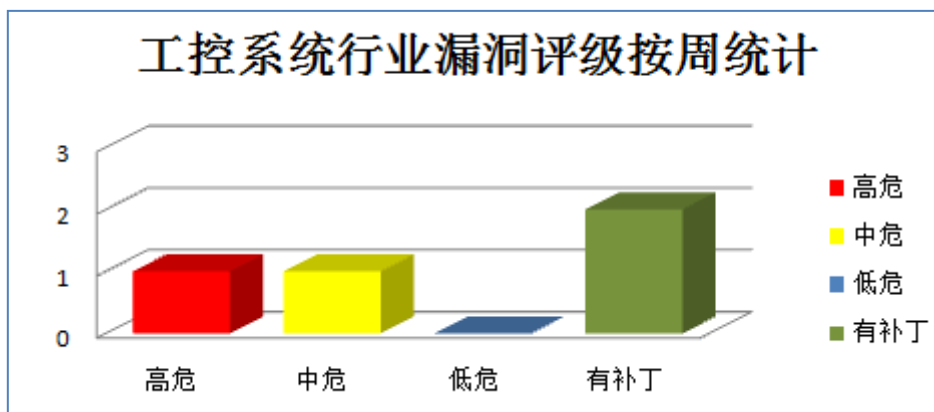


图 3 工控系统行业漏洞统计

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

3 月 10 日，微软发布了 2015 年 3 月份的月度例行安全公告，共含 14 项更新，修复了 Microsoft Windows、Internet Explorer、Exchange、Office 和 Server 软件中存在的 45 个安全漏洞。其中，5 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，获得敏感信息，或进行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft windows Adobe 字体驱动缓冲区溢出漏洞（CNVD-2015-01624、CNVD-2015-01623、CNVD-2015-01622、CNVD-2015-01621）、Microsoft windows kernel 本地权限提升漏洞（CNVD-2015-01620、CNVD-2015-01619）、Microsoft windows Adobe 字体驱动内存信息泄露漏洞（CNVD-2015-01627、CNVD-2015-01626）。其中，除“Microsoft windows Adobe 字体驱动内存信息泄露漏洞（CNVD-2015-01627、CNVD-2015-01626）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了其余漏洞的修补程序。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/3592>

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。本周，上述产品被披露存在拒绝服务和内存错误引用漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome Blink 拒绝服务漏洞（CNVD-2015-01502、CNVD-2015-01510）、Google Chrome Blink 内存错误引用漏洞（CNVD-2015-01547、CNVD-2015-01516、CNVD-2015-01511、CNVD-2015-01512）、Google Chrome Skia 拒绝服务漏洞（CNVD-2015-01509、CNVD-2015-01508）。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-2015-01502>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01510>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01547>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01516>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01511>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01512>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01509>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01508>

3、HP 产品安全漏洞

HP Point of Sale PCs Running Windows with OPOS Drivers 是美国惠普（HP）公司的一套运行于惠普销售点终端机 Windows 操作系统中的 OPOS 驱动程序。本周，上述产品被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：HP Point of Sale PCs Running Windows with OPOS Drivers 任意代码执行漏洞（CNVD-2015-01601、CNVD-2015-01600、CNVD-2015-01599、CNVD-2015-01598、CNVD-2015-01597、CNVD-2015-01596、CNVD-2015-01595、CNVD-2015-01594）。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-2015-01601>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01600>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01599>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01598>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01597>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01596>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01595>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01594>

4、Cisco 产品安全漏洞

Cisco IOS XR 是美国思科（Cisco）公司的 IOS 软件系列中的一套完全模块化、分布式的网络操作系统。Cisco IOS 是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco Secure Access Control Server（ACS）是美国思科（Cisco）公司的一款安全访问控制服务器。该服务器为思科智能信息网络提供基于身份的全面的访问控制解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Cisco IOS XR SNMPv2 实现拒绝服务漏洞、Cisco IOS Autonomic Networking Infrastructure 功能存在未明漏洞、Cisco IOS XR 拒绝服务漏洞（CNVD-2015-01497）、Cisco IOS Authentication Proxy 功能存在未明漏洞、Cisco IOS 和 IOS XE RADIUS 实现拒绝服务漏洞、Cisco Secure Access Control Server 任意代码执行漏洞。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-2015-01499>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01498>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01497>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01496>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01495>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01494>

5、Comsenz SupeSite CMS 任意代码执行漏洞

Comsenz SupeSite CMS 是中国康盛 (Comsenz) 公司的一套内容管理系统 (CMS)。本周, Comsenz SupeSite CMS 被披露存在综合评级为“高危”的任意代码执行漏洞。攻击者可利用该漏洞在受影响应用程序上下文中执行任意代码。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-2015-01587>

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-2015-01488	多个 Solarwinds 产品 core Orion 存在多个 SQL 注入漏洞	高	用户可以联系供应商获得补丁信息: http://www.solarwinds.com
CNVD-2015-01487	Webshop hun SQL 注入漏洞	高	暂无
CNVD-2015-01500	Symantec NetBackup OpsCenter 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 补丁获取链接: http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvaid=security_advisory&year=&suid=20150302_00
CNVD-2015-01517	libFLAC 'src/flac/encode.c'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://libzplay.sourceforge.net/FLAC.html
CNVD-2015-01521	GNOME librest 'rest_proxy_call_get_url()'内存破坏漏洞	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://wiki.gnome.org/Projects/LibreSt
CNVD-2015-01523	Request Tracker 远程拒绝服务漏洞	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://requesttracker.wikia.com/wiki/HomePage

CNVD-2015-01530	libgtk2-perl 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： https://packages.qa.debian.org/libg/libgtk2-perl.html
CNVD-2015-01529	VLC Media Player 'audio.c'堆缓冲区溢出漏洞	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://git.videolan.org/?p=vlc.git;a=commit;h=a3a150b91f09620dc0d81c22db591a20faf4b2a5
CNVD-2015-01543	ShareLaTeX 远程命令注入漏洞	高	用户可以联系供应商获得补丁信息： https://www.sharelatex.com/
CNVD-2015-01538	WebGate eDVR Manager ActiveX Controls 存在多个缓冲区溢出漏洞	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://www.symantec.com/products-solutions/

表 3 部分高危漏洞列表

小结：本周，微软发布了 2015 年 3 月份的月度例行安全公告，共含 14 项更新，修复了 Microsoft Windows、Internet Explorer、Exchange、Office 和 Server 软件中存在的 45 个安全漏洞。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，获得敏感信息，或进行拒绝服务攻击。此外，Google、HP、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发起拒绝服务攻击或执行任意代码。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在受影响应用程序上下文中执行任意代码。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、phpMyAdmin 修补 phpMyAdmin 产品漏洞

phpmyadmin 是 MySQL 数据库的在线管理工具，主要功能包括在线创建数据表、运行 SQL 语句、搜索查询数据以及导入导出数据等。

本周，phpmyadmin 修补了上述产品存在信息泄露漏洞，避免攻击者利用漏洞获取敏感信息。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/56068>

本周要闻速递

1. WordPress SEO 插件曝高危 SQL 注入漏洞

WordPress SEO by Yoast 插件是 WordPress 平台下非常流行的 SEO 插件,看其在 Yoast 网站上高达 1400 万次的下载量就知道了。该漏洞是 WordPress 漏洞扫描器 “WPScan” 开发者 Ryan Dewhurst 发现——1.7.3.3 之前版本的 WordPress SEO by Yoast 都会受到 SQL 盲注 web 应用程序漏洞的影响。SQL 注入漏洞之所以被标记为高危漏洞,是因为它可能会导致大量数据和敏感信息泄露。通常,在 SQL 注入攻击中,攻击者会通过客户端在应用程序中输入一个畸形的 SQL 请求。该漏洞仅影响 WordPress 内部用户,因为该漏洞存在于 admin/class-bulk-editor-list-table.php 文件中,而此文件只有 WordPress 管理员、编辑和特权作者才能访问。

参考链接: <http://www.freebuf.com/news/60715.html>

2. Dropbox SDK 存在远程利用漏洞,已紧急修复

Dropbox 的开发人员近日修复了安卓版 Dropbox SDK 存储应用程序上的一个远程利用漏洞,攻击者利用该漏洞可未经用户同意直接把应用程序和 Dropbox 账户连接。只要用户安装的应用程序使用了含有漏洞的 Dropbox SDK,则其敏感信息就可能被攻击者窃取。参考链接: <http://www.freebuf.com/news/60684.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