国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 06 月 08 日-2015 年 06 月 14 日 **2015 年第 24 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 145 个，其中高危漏洞 66 个、中危漏洞 65 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 124 个。本周收录的漏洞中，已有 119 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“WordPress 插件 XCloner 远程命令执行漏洞”、“PCRE ‘match()’函数栈缓冲区溢出漏洞”等零日漏洞，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 145 个漏洞。报送情况如表 1 所示。其中，奇虎、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 Bridge Security Research Lab、乌云、漏洞盒子、四川大学信息安全研究所及白帽子向 CNVD 提交了 539 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎	286	286
天融信	135	3
启明星辰	131	0
安天实验室	131	0
恒安嘉新	74	0

绿盟科技	24	0
乌云	222	222
漏洞盒子	3	3
High-Tech Bridge Security Research Lab	5	5
四川大学信息安全研究所	1	1
CNCERT 新疆分中心	3	3
CNCERT 安徽分中心	1	1
CNCERT 黑龙江分中心	1	1
个人	14	14
报送总计	1031	539
录入总计	145（去重）	539

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、SysAid、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	Microsoft	44	30%
2	SysAid	9	6%
3	Cisco	8	6%
4	IBM	7	5%
5	Linux	7	5%
6	Adobe	6	4%
7	WordPress	5	3%
8	PCRE	3	2%
9	Drupal	2	1%
10	其他	54	38%

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 145 个漏洞。其中应用程序漏洞 84 个，操作系统漏洞 24 个，WEB 应用漏洞 21 个，网络设备漏洞 12 个，数据库漏洞 2 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	84
操作系统漏洞	24
WEB 应用漏洞	21
网络设备漏洞	12
数据库漏洞	2
安全产品漏洞	2

表 3 漏洞按影响类型统计表

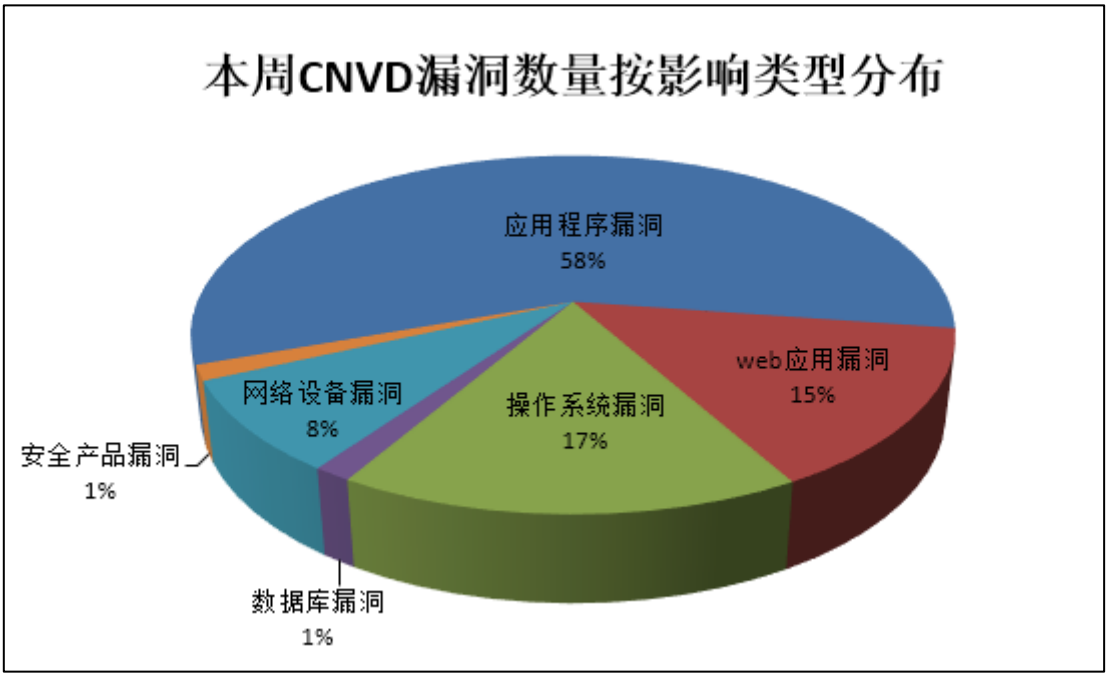

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 3 个电信行业漏洞，1 个移动互联网行业，2 个工控系统行业漏洞（如下图表所示）。其中，“Beckhoff IPC Diagnostics 任意用户创建漏洞”的综合评级为“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-2015-03768	多款 Buffalo 路由器任意命令执行漏洞	中	是

电信	CNVD-2015-03677	多款 IBM Flex System 产品 HTTP 响应拆分漏洞	中	是
电信	CNVD-2015-03676	多款 IBM 产品跨站请求伪造漏洞	中	是
移动互联网	CNVD-2015-03669	Brandon Bowles Open Explorer application 目录遍历漏洞	中	是
工控系统	CNVD-2015-03767	Beckhoff IPC Diagnostics 任意用户创建漏洞	高	是
工控系统	CNVD-2015-03655	IDS RTU 850 Series 目录遍历漏洞	高	否

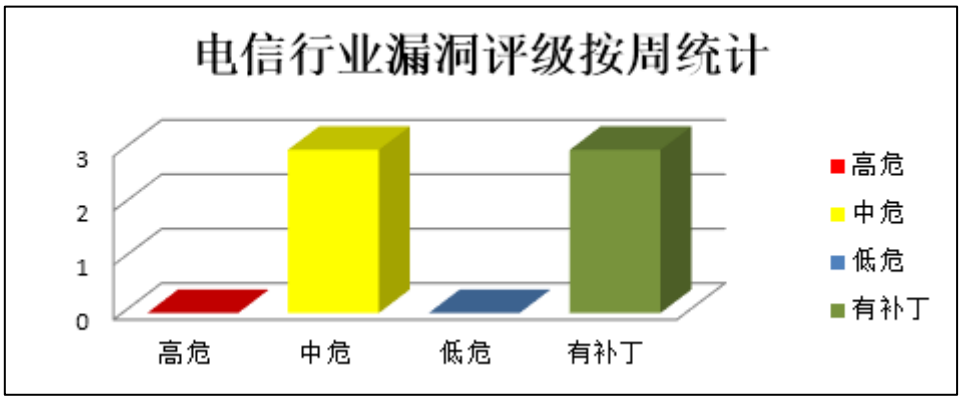

图 1 电信行业漏洞统计

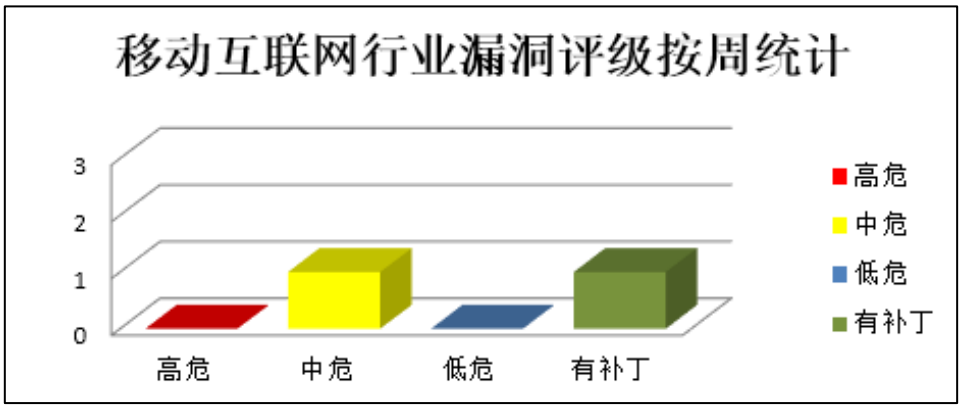

图 2 移动互联网行业漏洞统计

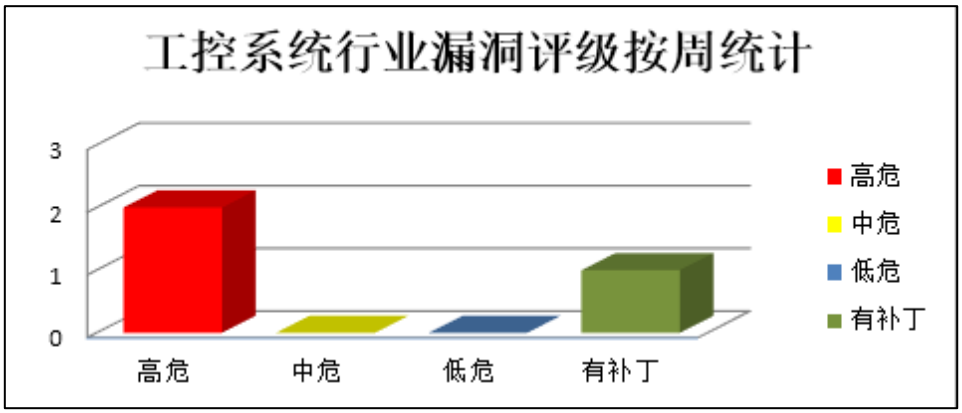

图 3 工控系统行业漏洞统计

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

6 月 9 日，微软发布了 2015 年 6 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Exchange Server 中存在的 45 个安全漏洞。其中，2 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。

CNVD 收录的相关漏洞包括：Microsoft Windows Media Player 远程代码执行漏洞、Microsoft Windows Kernel 'Win32k.sys'本地权限提升漏洞（CNVD-2015-03730）、Microsoft Windows Kernel 'Win32k.sys'内存破坏权限提升漏洞、Microsoft Windows Common Controls 内存错误引用漏洞、Microsoft Office 未初始化内存错误漏洞、Microsoft Office 内存破坏漏洞（CNVD-2015-03736）、Microsoft Office 任意代码执行漏洞（CNVD-2015-03735）、Microsoft Windows 内核 brush 对象内存错误引用漏洞。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。

参考链接：http://www.cnvd.org.cn/webinfo/show/3643

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该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或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存破坏任意代码执行漏洞、Adobe Flash Player ASLR 防护绕过漏洞、Adobe Flash Player 同源策略绕过信息泄露漏洞（CNVD-2015-03774）、Adobe Flash Player 跨站请求伪造漏洞、Adobe Flash Player 同源策略绕过信息泄露漏洞、Adobe Flash Player SWF 文件处理本地信息泄露漏洞。其中，“Adobe Flash Player 内存破坏任意代码执行漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Adobe Flash Player SWF 文件处理本地信息泄露漏洞”外，其余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-2015-03773
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03777
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03774
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03776
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03775
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03674

3、 Linux 产品安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，该产品被披露存在信息泄露、拒绝服务漏洞。远程攻击者利用漏洞可提交特殊的数据包，获取内核内存中的敏感信息，或造成拒绝服务。

CNVD 收录的相关漏洞包括：Linux Kernel 本地信息泄露漏洞（CNVD-2015-03744）、Linux kernel OZWPAN 驱动程序拒绝服务漏洞（CNVD-2015-03717、CNVD-2015-03716、CNVD-2015-03715、CNVD-2015-03714）、Linux Kernel ‘fs/udf/inode.c’空指针引用拒绝服务漏洞 、Linux Kernel UDF File System 拒绝服务漏洞。其中，“Linux kernel OZWPAN 驱动程序拒绝服务漏洞（CNVD-2015-03717、CNVD-2015-03716、CNVD-2015-03715、CNVD-2015-03714）”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-2015-03744

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03717

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03716

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03715

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03714

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03662

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03661

4、SysAid Help Desk 安全漏洞

SysAid Help Desk 是一套基于 Web 的 IT 管理软件。本周，该产品被披露存在文件上传、SQL 注入、目录遍历、拒绝服务漏洞。攻击者可利用漏洞获取敏感信息、进行跨站攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：SysAid Help Desk 拒绝服务漏洞、SysAid Help Desk 任意文件上传漏洞、SysAid Help Desk 目录遍历漏洞、SysAid Help Desk 敏感信息泄露漏洞、SysAid Help Desk 硬编码密钥漏洞、SysAid Help Desk SQL 注入漏洞、SysAid Help Desk 内置密码漏洞、SysAid Help Desk 限制绕过漏洞。其中“SysAid Help Desk 限制绕过漏洞、SysAid Help Desk 目录遍历漏洞、SysAid Help Desk 拒绝服务漏洞”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-2015-03766

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03750

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03749

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03747

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03746

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03745

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03712

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03753

5、PCRE 'match()'函数栈缓冲区溢出漏洞

PCRE（Perl Compatible Regular Expressions）是一个使用 C 语言编写的开源正则表达式函数库。本周，PCRE 'match()'函数被披露存在综合评级为“高危”的栈缓冲区溢出漏洞。攻击者利用该漏洞可执行任意代码，或发起拒绝服务攻击。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-2015-03757

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-2015-03764	Wing FTP Server 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，请用户及时下载更新：http://www.wftpserver.com/
CNVD-2015-03755	Drupal Novalnet Payment 模块 SQL 注入漏洞	高	暂无
CNVD-2015-03748	Redis EVAL Lua 沙箱安全绕过漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请用户及时下载更新：https://raw.githubusercontent.com/antirez/redis/3.0/00-RELEASENOTES
CNVD-2015-03759	Novell ZENworks Configuration Management Remote Management 组件目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.novell.com/support/kb/doc.php?id=7005573
CNVD-2015-03760	PHP ‘SoapClient's __call()’函数任意代码执行漏洞	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：http://php.net/
CNVD-2015-03771	JSPMyAdmin 存在多个漏洞	高	暂无
CNVD-2015-03767	Beckhoff IPC Diagnostics 任意用户创建漏洞	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：http://ftp.beckhoff.com/download/document/IndustPC/Advisory-2015-001.pdf
CNVD-2015-03682	WordPress 插件 XCloner 远程命令执行漏洞	高	暂无

CNVD-2015-03667	CA Common Services 变量处理本地权限提升漏洞	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.ca.com/irj/portal/anonymous/phpsbpldgpg
CNVD-2015-03709	WebDrive 存在多个缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，微软发布了 6 月安全公告，修复了 Microsoft Windows、Internet Explorer、Office 和 Exchange Server 中存在的 45 个漏洞。攻击者可利用漏洞执行远程代码，提升权限。此外，Adobe、Linux、SysAid Help Desk 被披露存在多个安全漏洞，利用漏洞可获取敏感信息、进行跨站攻击、执行任意代码或发起拒绝服务攻击。另外，PCRE（Perl Compatible Regular Expressions）被披露存在一个高危零日漏洞，攻击者利用该漏洞可执行任意代码，或发起拒绝服务攻击。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、Apple 修补 MAC 漏洞

MAC 是 apple 公司自主研发的操作系统。

本周，HP 修补了上述产品存在的固件漏洞，避免攻击者通过 Safari 等其他远程向量利用此漏洞，安装 EFI rootkit，更新 flash ROM 内容等。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/59469

本周要闻速递

1. iOS 新漏洞可轻易窃取 iCloud 密码

安全研究人员近日发布了一份漏洞利用代码。这份代码表明，攻击者可以通过足以以假乱真的钓鱼，轻易窃取使用最新 iOS 版本的 iCloud 密码。目前，苹果方面并未做出任何回应。而安全研究人员的建议是，不要输入任何帐号密码，而是直接按下取消按钮。因为如果是正常的提示框，在按下 OK 或取消按钮之前，它不允许用户进行任何其他操作。而伪造的密码提示并不是模态的，所以如果在显示密码提示框时按下 home 键设备回到了主屏幕，那么这就表明这个密码提示是不可信的。

参考链接：http://www.cu-market.com.cn/hgjj/20150612/1634322021.html

2. Mozilla 提升安全漏洞奖金上限 1 万美元

近日 Mozilla 公司为激励更多的白客和安全专家加入到 Client Bug Bounty 项目中来，

帮助修复软件漏洞，选择最大漏洞奖金上限提升至 1 万美元。而发现的漏洞必须是比较重要的漏洞，远程可执行代码、导致权限提升或者信息泄漏的安全漏洞。此外为防止漏洞的潜在风险，程序员并不要求在报告问题中提供自己的 BUG 代码，Mozilla 基金会的员工无权利提交报告。

参考链接：http://article.pchome.net/content-1817567.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